institute of development studies

Surveillance Law in Africa: a review of six countries

Tony Roberts (editor)

Authors: Tony Roberts, Abrar Mohamed Ali, Mohamed Farahat, Ridwan Oloyede and Grace Mutung'u.

The Institute of Development Studies (IDS) delivers world-class research, learning and teaching that transforms the knowledge, action and leadership needed for more equitable and sustainable development globally.

For more information visit: www.ids.ac.uk

Research Report

Surveillance Law in Africa: a review of six countries

Editor: Tony Roberts

First published by the Institute of Development Studies in October 2021

Suggested citation:

Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) *Surveillance Law in Africa: a review of six countries*, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.059**

ISBN: 978-1-78118-865-1

DOI: **10.19088/IDS.2021.059**

A catalogue record for this publication is available from the British Library

Funding acknowledgements

This paper is supported by funding from Omidyar Network. The creation of the African Digital Rights Network (ADRN) was funded by the Global Challenge Research Fund (GCRF). The network brings together activists, analysts and researchers from seven African countries. Network members share a commitment to opening online democratic space and to enabling citizens to freely exercise their digital rights including the rights to privacy and to freedom of opinion and speech. Members of ADRN, funded by Omidyar Network, have worked together on this paper to analyse surveillance law in African countries.

Other acknowledgements

The authors would like to gratefully acknowledge reviewer feedback from, Karishma Banga, Tanja Bosch, Becky Faith, Jo Howard, George Karekwaivanane, Pedro Prieto Martin, Nanjala Nyabola, Sam Phiri and Anand Sheombar.

Copy-editor: James Middleton; Kathryn O'Neill; Rosalind Cook

Designer: Blossom Carrasco

Proofreader: Karen Stubbs

Brighton, BN1 9RE, United Kingdom

+44 (0)1273 915637
ids.ac.uk

IDS is a charitable company limited by guarantee and registered in England
Charity Registration Number 306371
Charitable Company Number 877338

Contents

Executive summary

An expansion of state surveillance is underway that involves violations of citizens' privacy rights. This is happening despite explicit guarantees of these privacy rights in African constitutions, international human rights conventions and domestic laws. Governments are making large investments in new surveillance technologies, passing laws that expand their legal surveillance powers, and conducting illegal surveillance of journalists, judges, business rivals and opposition leaders.

Illegal state surveillance is being carried out with impunity. Among other examples, this report includes evidence of illegitimate state surveillance: of journalists and academics in Egypt; of business rivals and politicians in South Africa; of activists and lawyers in Sudan. The impunity of those conducting illegal surveillance, is evidenced by the absence of any prosecutions of those acting outside of the law to violate citizens' constitutional privacy rights.

Surveillance law attempts to balance privacy rights with the need to enable legal surveillance of individuals suspected of committing the most serious crimes. Surveillance law provides a means to ensure that surveillance is narrowly targeted, while protecting citizens' rights by defining in law privacy and due process safeguards, transparency and independent oversight mechanisms. However, little research currently exists about what legal provisions are in place across Africa and how legal frameworks compare with each other and with available guidelines.

This review provides the first comparative analysis of African legal surveillance frameworks. The study identifies nine core principles derived from existing guidelines as an analytical framework to identify opportunities to strengthen privacy protection, while narrowly targeting surveillance on the most serious crimes. Six detailed country reports are synthesised in this comparative analysis to produce a series of actionable recommendations for policy, practice and further research.

This report finds that existing surveillance law is failing to protect privacy rights, which are currently being eroded by six factors:

1. The introduction of new laws that expand state surveillance powers.
2. Lack of legal precision and privacy safeguards in existing surveillance legislation.
3. Increased supply of new surveillance technologies that enable illegitimate surveillance.
4. State agencies regularly conducting surveillance outside of what is permitted in law.

5. Impunity for those committing illegitimate acts of surveillance.
6. Insufficient capacity in civil society to hold the state fully accountable in law.

This report finds state violation of privacy rights occurs in all countries studied and that impunity exists for those conducting illegitimate surveillance. No prosecutions were recorded in any country for those state employees conducting illegitimate surveillance of citizens. Civil society activists are alarmed about evidence of surveillance creep, the normalisation of illicit surveillance and what they fear is a slow descent into digital authoritarianism.

How to improve surveillance legislation is clear. There is a high degree of consensus among scholars and international bodies about how to significantly improve existing surveillance law. This review recommends establishing a single surveillance law in each country. Surveillance law should require an independent judge to test all surveillance applications for reasonable grounds, legitimate aims, necessity and proportionality. Legislation must provide legal precision and define mechanisms for notification, transparency, oversight and legal punishments for illegitimate surveillance.

Legislation alone is insufficient. Unless the state adheres to the law, it has limited relevance. Our country reports suggest that holding governments accountable in law depends on a strong and active civil society. Raising public awareness about privacy rights and surveillance practices is a necessary precondition to mobilising the political will that is necessary for reform of the law and the ending of impunity. This requires sustained capacity building and coordinated action with journalists, lawyers, human rights activists, policymakers and other stakeholders. A systematic approach is necessary that includes – but goes beyond – reform of legislation.

Figure 1.1 provides a visual summary of the provisions of surveillance law in each country studied. This table is derived from the more comprehensive analysis contained in each of the full country reports included in this publication. Each of the full country reports contains sections addressing a specific area of privacy rights and that country's surveillance law framework.

Figure 1.1 Privacy Protections Provided in Surveillance Legislation

Figure 1.1 provides a visual summary of the provisions of surveillance law in each country studied. This table is derived from the more comprehensive analysis contained in each of the full country reports included in this publication. Each of the full country reports contains sections addressing a specific area of privacy rights and that country's surveillance law framework.

	EG*	KE	NG	SG	SA**	SD***
Competent judicial authority: a judge knowledgeable in digital technologies and human rights to assess and authorise requests to conduct surveillance from investigating agencies of the state.	◒	◒	●	●	●	◒
Legality: surveillance carried out only within parameters and by agencies specified in the legislation. The legislation criminalises all other surveillance and specifies penalties.	◒	◒	●	●	●	◒
Legitimate aim: law closely defines the only legitimate aims of surveillance e.g. prevention of terrorism or serious crime with a legal punishment of 10 or more years in jail.	◒	◒	●	●	●	◒
Reasonable grounds: judge must test whether there is a high degree of threat and a high probability that surveillance will produce evidence that removes the threat to a legitimate aim.	◒	●	●	●	●	◒
Necessary: judge must test whether surveillance is necessary to secure the evidence and that no other less invasive method is available to address legitimate aim.	◒	◒	●	●	●	○
Proportionality: judge must test whether proposed surveillance is limited in scope, and that the duration is in proportion to the evidence needed to remove the threat.	◒	◒	●	●	●	◒
Notification: at the earliest appropriate time the subject of surveillance should be notified of the occurrence to provide opportunity for legal appeal and due process.	○	○	○	○	○	○
Transparency: annual transparency reports should publicise number of requests, grounds, and authorisations to enable public accountability of process and public officials.	○	○	○	○	●	○
Independent oversight: public oversight mechanisms should be established to ensure transparency and accountability of surveillance practices.	○	○	○	○	●	○

* Although Egyptian law provides some partial protections the Emergency Law in place since 2017 removes all of these protections

** South Africa's RICA law provides most protections but parts of the law have been suspended by the constitutional court to add new protections

*** Although some protections are provided in Sudanese law the current National Securty law enables state agencies to override the protections

KEY

- ● Provided in legislation
- ◒ Partial provision
- ○ No provision in legislation

1. Introduction

The right to privacy and to private communications is a fundamental human right that is enshrined in African constitutions, international human rights conventions and domestic laws. All surveillance is a violation of these privacy rights. States argue that on occasion it is necessary to violate privacy rights to prevent serious crimes such as terrorist attacks. The large power imbalance between the state and citizens and the secretive nature of surveillance creates the risk of abuse. Examples in this study show that states use surveillance powers to spy on journalists, business rivals, opposition politicians and activists in ways that threaten open democracy.

Surveillance law can provide a mechanism to protect privacy rights, while enabling the state to conduct narrowly targeted surveillance on those suspected of the most serious crimes. Protections can be built into law to protect against arbitrary or mass surveillance. The intention is to narrowly target surveillance so that citizens' fundamental human rights are infringed as little as possible. Surveillance law can, for example, require prior authorisation of surveillance by a judge and require specific safeguards, transparency and oversight mechanisms to prevent inconsistent application of the law or any abuse of surveillance powers.

State surveillance is not new but has dramatically expanded in the digital era. Colonial powers used surveillance to enable extraction of taxes and to monitor the struggle for independence. In recent years, analogue surveillance has been digitalised and automated, making mass surveillance possible. This has happened against a backdrop of 15 consecutive years of reductions in democratic freedoms worldwide (Freedom House 2021) and shrinking civic space globally (CIVICUS 2020). The violation of human rights occurs in many countries, but the threat is arguably greatest in fragile democracies: those with weak legal and regulatory oversight, poor institutional protections and where levels of awareness about privacy rights and surveillance practices are lowest. There are relatively few studies on new surveillance technologies and practices in Africa (Roberts and Mohamed Ali 2021). This report examines existing surveillance law and practice in six African countries and assesses them against international law. It identifies opportunities to better balance the protection of citizens' privacy with the state's need to conduct narrowly targeted surveillance. This is the first such comparative analysis of African legal surveillance frameworks.

The Cambridge Analytica scandal, Snowden revelations and Pegasus spyware cases have provided copious evidence that governments regularly conduct surveillance on citizens (Ekdale and Tully 2020; Courage Foundation 2015; Amnesty 2021). Our study evidences a rapid expansion in the sale of new surveillance technologies to African countries by companies from the US, China, Europe and Israel (Duncan 2018; Feldstein 2019; Jili 2020; Amnesty 2021; Roberts 2021). The expansion of the technical means to conduct mass surveillance alongside the contraction of democratic space has raised concerns about what Freedom House (2018) has called a descent into 'digital authoritarianism'. There has been no systematic attempt to document which companies are providing what surveillance technologies to African governments and with what effect (Roberts and Mohamed Ali 2021). This report is one of the first attempts to document this expansion of surveillance technologies across Africa. Further research is needed in this area if actions to mitigate and curtail illegitimate surveillance are to be successful.

This report reviews the existing legal frameworks for surveillance in Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan. The countries selected as case studies include examples from four main regions and three main language groups. The six country reports summarise the existing legislation, safeguards and practice in each country and compare this against three international frameworks. The frameworks used are the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2013), the UN Draft Instrument on Government-led Surveillance and Privacy (UNHCHR 2018a) and the African Commission (2019) Declaration of Principles of Freedom of Expression and Access to Information in Africa. These three guiding documents are complementary and are referred to collectively in this review as 'the Principles'.

The rest of this report proceeds as follows: section 2 provides essential background on privacy rights and surveillance law before the methodological approach is outlined in section 3; section 4 reviews existing literature on underlying principles to guide surveillance law to produce the framework of analysis used in this review; section 5 provides brief visual summaries of the six fully detailed reports included at the end of this publication; section 6 highlights the main findings of the research by analysing the six country reports using this framework, before presenting a set of conclusions and recommendations in section 7. This is followed by the full country reports from Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan.

2. Background

Privacy rights

Citizens have reason to value privacy in their own homes, in their business correspondence and personal communications. Reflecting the high value that societies generally attach to it, the right to privacy is enshrined in the constitution of many countries, guaranteed in international conventions and explicitly protected in many domestic laws. This universal human right to privacy applies whether a person is alone or with others, in a private home or a public place, corresponding by any medium, and whether they are online or offline (Privacy International 2019).

Privacy itself is a fundamental right, but it is also instrumental in securing other rights including the rights to freedom of speech, opinion, affiliation and assembly (Bernal 2016). Without privacy it is often not practical or safe to organise political opposition, compete commercially or otherwise develop alternatives to existing policies, dominant narratives or experienced injustice. As such, the right to privacy is central to democracy and is explicitly recognised in international human rights law including the Universal Declaration of Human Rights (UN 1948), the International Covenant on Civil and Political Rights (UN 1966) and the Declaration of Principles of Freedom of Expression and Access to Information in Africa, hereafter referred to in this report as the 'African Declaration' (African Commission 2019).

The right to privacy of communication is a universal right guaranteed to all in international law. Article 12 of the Universal Declaration of Human Rights states that: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (UN 1948). This was reinforced by Article 17 of the International Covenant on Civil and Political Rights (UN 1966), which requires states to protect and promote the right to privacy for all individuals without discrimination. The Cairo Declaration on Human Rights in Islam (Islamic Conference 1990) goes further by specifically mentioning surveillance, saying, 'It is not permitted to spy on him [sic.], to place him under surveillance' and requiring that 'The State shall protect him from arbitrary interference'. More recently the UN Human Rights Council has passed resolutions on 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (UN 2016) and the Right to Privacy in the Digital Age (UNHCHR 2018a), which add clarity around the need to limit surveillance in order to protect the fundamental human right to privacy.

The African Commission (2019) Declaration of Principles on Freedom of Expression and Access to Information explicitly prohibits surveillance except as authorised in legislation. The Declaration specifies the right to anonymity online and explicitly prohibits surveillance outside of a legal framework. The African Declaration requires prior authorisation of any surveillance by an impartial and independent court. Surveillance is only allowed to secure a 'legitimate aim', where there is 'reasonable suspicion' that a serious crime has been or is about to be committed. The African Declaration also stipulates the need to put in place appropriate safeguards against arbitrary surveillance by requiring the authorising judge to assess whether the scope and time frame of proposed surveillance is 'legal, necessary, and proportionate' to the legitimate aim. These principles and protections are discussed in more detail in the sections that follow.

Surveillance law

Although guaranteed in law, the right to privacy is not absolute. Although conventions may 'guarantee' privacy and constitutions make it 'inviolable', states argue there are circumstances when it is necessary to violate one person's rights in order to protect the rights of others. A government might, for example, give itself the power to violate a suspected terrorist's right to privacy in order to prevent a terrorist attack that threatens the lives of many. However, as this report will show, the danger exists that a present or future government might use surveillance powers granted in order to protect against terrorism to spy on political opponents, gain commercial advantage, or stifle progressive social or political change. Surveillance law attempts to provide checks and balances to enable narrowly targeted surveillance, while protecting against arbitrary or mass surveillance.

State surveillance is defined in this report as any observing, listening, monitoring or recording by a state or its agents to track citizen's movements, activities, conversations, communications or correspondence, including the recording of metadata.

Surveillance is always a relationship of power in which the watcher covertly gains advantage at the expense of the fundamental rights of those being watched. The covert nature of surveillance and the imbalance of power between the watcher and the watched provide significant opportunity for the abuse of power with impunity. Therefore, safeguards are necessary to limit the potential for arbitrary and illegitimate use of surveillance, to make its use transparent and power holders accountable. Introducing clear limits and transparent safeguarding mechanisms into the text of surveillance legislation is one potential means to curb arbitrary surveillance and balance citizens' right to privacy with the need for narrowly targeted surveillance.

Artificial intelligence and automated algorithmic searching of digital communications increase the potential scale and speed of covert monitoring, making mass surveillance practically possible. Until relatively recently, the scope of surveillance was practically limited by resource constraints. Communications interception was a labour-intensive analogue process. Several people were required to track, intercept, monitor and analyse each surveillance target. It is now possible to monitor citizens' internet and mobile communications digitally by searching for keywords in ways that make mass surveillance more efficient and affordable.

African governments are making major investments in a wide range of surveillance technologies. This report documents that African governments are creating laws that force mobile and internet companies to capture and store all citizen's communications for analysis by state agencies. In some countries, all banking and electronic financial transactions are similarly available to the state. In all countries studied, mobile phone SIM card registration is mandatory. Compulsory digital identification (ID) systems are being introduced in some countries and major investments are being made in closed circuit television (CCTV), car licence plate and facial recognition systems. Being able to track an individual's real-time movements, transactions, email, voice and social media communications provides a powerful basic infrastructure for state surveillance. This report is one of the first attempts to document this expansion of surveillance technologies across Africa, but more research is necessary in this area.

Privacy rights advocates argue that the expansion of mass surveillance by states is not lawful and that it is neither necessary nor proportionate to the legitimate aim of preventing serious crime. Following revelations in 2013 by US National Security Agency whistle-blower Edward Snowden that the US and UK governments were conducting mass surveillance of citizens, courts in both countries upheld that the practices were illegal and unconstitutional. Yet these technologies are now being exported to African states. Globally, there has been broad agreement that there is a need to tighten surveillance laws to reflect the new digital environment, protect fundamental privacy rights and make possible targeted surveillance that minimises privacy violation. This review contributes actionable recommendations towards meeting those aims.

The report details existing legal surveillance frameworks in six African countries and measures them against available guidance for best practice in surveillance law (these guidance documents are analysed in section 4). The next section explains the methodology adopted in this study.

3. Methodology

This research provides the first comparative analysis of African legal surveillance frameworks. The study uses nine core elements from existing international principles as a framework to identify opportunities to strengthen privacy protection and narrowly target surveillance. The guiding research question was: 'What legal provisions exist to protect privacy and ensure narrowly targeted surveillance in six African countries?' The objective was to understand existing strengths, identify improvement opportunities and produce recommendations for policy, practice and further research. This section explains the research approach adopted.

Six countries were selected to represent a variety of geographical regions and language groups. We sought to include countries that provide some contrast of surveillance practices and legal frameworks. On a practical level, the selection also included the funder's focal countries in the region. The final decision was pragmatically influenced by our ability to identify and secure the services of legal scholars with relevant expertise within the timeframe and budget available.

The researchers were legal and digital scholars based in five African countries and the UK. The research was carried out between April and August 2021. Due to resource and Covid-19 pandemic restrictions, the study was entirely desk-based qualitative analysis of primary legislation and secondary sources. Each country report author was required to answer the same 12 research questions in order to provide the basis for cross-country comparison. These 12 questions provide the structure for the six full country reports included in this publication.

The analytical framework was based on agreed international principles. The country report authors were originally asked to compare domestic surveillance laws in six African countries with those existing in countries in Europe, the UK and the US. Ultimately, comparison with existing legal frameworks in other countries did not prove to be as useful analytically as comparison with the available Principles (detailed in section 4). The existing frameworks for surveillance law in the Europe, the UK and the US were themselves problematic in both their content and application. These issues are summarised in the remaining paragraphs in this section.

After the 9/11 terrorist attacks in 2001, the US rushed through legislation giving the state extensive new surveillance powers. In the US, The USA Patriot Act was hastily introduced within 45 days of 9/11 making it legal for the US government to spy on its own citizens and globally. The

availability of new technologies provided the opportunity to automate some communications interception tasks using artificial intelligence to algorithmically search and analyse part of the surveillance process, making mass surveillance possible. Although the case for new surveillance powers was premised on the need to prevent terrorism, in fact the overwhelming majority of convictions secured with PATRIOT Act surveillance have been unrelated to terrorism (ACLU 2021). This has raised concerns that surveillance powers ushered in using the justification of national security are put to other uses.

The Snowden revelations in 2013 provided copious evidence that the US and UK governments were routinely carrying out mass surveillance that far exceeded their legal powers (Snowden 2015). Following public outcry at the mass surveillance of citizens by the state, and court cases in both the UK and US ruling that the state had acted illegally (Crocker 2015), new laws were promised to remedy the situation. In the US, the USA Freedom Act was originally intended to correct the weaknesses of the Patriot Act and prevent the kind of illegal mass surveillance revealed by Snowden. However, the Freedom Act was watered down as it passed through the legislative process and civil rights organisations have lamented that the final legislation failed to introduce any meaningful restraints on surveillance powers and actually extended and legitimated some forms of mass surveillance (Bradford Franklin 2019).

A similar pattern occurred in the UK. Public shock at the Snowden revelations and the ensuing media furore created momentum for new legal protections. However, the much-amended final legislation (Investigatory Powers Act 2016) was 'one of the most extreme surveillance laws ever introduced in a democratic country' according to lawyers and human rights organisation Article 19 (2019). The Investigatory Powers Act – dubbed the 'Snooper's Charter' by privacy campaigners – 'legitimizes mass surveillance. It is the most intrusive and least accountable surveillance regime in the West' (Snowden 2015).

For these reasons, our researchers did not find US or UK law a useful reference point for assessing African surveillance law. The legal framework for surveillance is arguably better in some European countries than the US and UK. For example, the main surveillance law in Germany, called the G10 Act, makes mass surveillance illegal due to the threat that it presents to journalists, lawyers and their clients. The same law also protects the right to anonymity prohibiting the state from breaking encryption (Gerhold *et al.* 2017). The German legislation is not perfect – with deficiencies around transparency and proportionality – but a strong civil society, and relatively

independent media and courts, mean that such limitations can be legally challenged and reformed.

Our research team was resistant to the idea that African law should always be compared against US and European laws. This was especially the case given the problematic nature of the examples of the US and UK. Ultimately, report authors found that the International Principles, UN Draft Instrument and African Declaration were more useful frameworks for analysing surveillance law in the six countries studied. These three documents are grounded in the same human rights language as is found in their national constitutions and domestic law. As such, the researchers found that the documents provided a solid ethical and contextually relevant basis for assessing the strengths of existing legal frameworks in their respective countries. These Principles are discussed in detail in the next section.

4. Analytical approach

This section outlines a series of guidance documents and principles for surveillance law that have been developed and agreed by a wide group of stakeholders and which are used to support countries aiming to balance privacy rights and the need for narrowly targeted surveillance.

The International Principles

In 2013, civil society organisations concerned about the threat to human rights posed by digital surveillance collectively authored a set of International Principles on the Application of Human Rights to Communications Surveillance (EFF 2014). Privacy International, the Open Rights Group, Electronic Frontier Foundation and Association of Progressive Communications were among those coordinating the drafting, with over 600 organisations signing the International Principles.[1] The International Principles outline among other things the importance of prior authorisation of surveillance by a competent judicial authority; the testing of applications by a judge for legitimate aims, reasonable grounds, legality, necessity and proportionality; and the importance of subject notification, transparency reports and independent oversight (as illustrated in Figure 1.2).

1 https://necessaryandproportionate.org/principles/

Figure 1.2 Principles of surveillance law

Competent Judicial Authority: a judge knowledgeable in digital technologies and human rights to assess and authorise requests to conduct surveillance from investigating agencies of the state

Legality: surveillance carried out only within parameters and by agencies specified in the legislation. The legislation criminalises all other surveillance and specifies penalties

Legitimate Aim: law closely defines the only legitimate aims of surveillance e.g. prevention of terrorism or serious crime with a legal punishment of 10 or more years in jail

Reasonable Grounds: judge must test whether there is a high degree of threat to a legitimate aim and a high probability that surveillance will produce evidence that removes the threat

Necessary: judge must test whether surveillance is necessary to secure the evidence and that

no other less invasive method is available to address legitimate aim

Proportionality: judge must test whether proposed surveillance is limited in scope, and that the duration is in proportion to the evidence needed to remove the threat.

Notification: at the earliest appropriate time the subject of surveillance should be notified of the occurrence to provide opportunity for legal appeal and due process

Transparency: annual transparency reports should publicise number of requests, grounds, and authorisations to enable public accountability of process and public officials

Independent oversight: public oversight mechanisms should be established to ensure transparency and accountability of surveillance practices

Source: Authors – adapted from EFF (2014).

The UN Draft Legal Instrument

In 2018, a group of experts from global technology companies, civil society organisations, law enforcement and intelligence agencies, and universities came together under the auspices of the UN Special Rapporteur on the Right to Privacy to produce the Draft Legal Instrument on Government-led Surveillance and Privacy (UNHCHR 2018a). The Draft Legal Instrument is a comprehensive guide to legislation that enables narrowly targeted surveillance with safeguards for privacy rights. The Draft Legal Instrument provides a clear guide for drafting and assessing surveillance legislation that complies with international law on human rights.

The African Declaration

In 2019, many of the elements of the International Principles and the UN Draft Legal Instrument were incorporated into section 41 of the African Commission's (2019) Declaration of Principles of Freedom of Expression and Access to Information in Africa (African Declaration), as illustrated in Box 1.1. The founding charter of the African Commission includes a responsibility to promote human rights, in part by formulating and laying down principles to help African states draft legislation that is consistent with international human rights law. Mindful of this responsibility and of the rapidly evolving digital landscape, the 2019 declaration sought to update the previous 2002 declaration as major new issues had emerged, including in relation to digital information and mobile and internet technologies (Mute 2019).

Box 1.1 African Commission (2019) Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019.

Principle 41. Privacy and communication surveillance

1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.
2. States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:
    a. the **prior authorisation** of an independent and **impartial judicial authority;**
    b. due process **safeguards;**
    c. specific limitation on the time, manner, place and scope of the surveillance;
    d. **notification** of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
    e. proactive **transparency** on the nature and scope of its use; and
    f. effective monitoring and regular review by an **independent oversight mechanism.**

Source: adapted from EFF (2014).

The Principles

There is a high degree of consensus between the guidance contained in the International Principles, UN Draft Legal Instrument and African Declaration. All three documents emphasise the importance of guarding against indiscriminate or mass surveillance and are clear about the need to ensure any surveillance is narrowly targeted only on legitimate aims. The International Principles, UN Draft Legal Instrument and African Declaration all agree prior authorisation for surveillance by a judge should test that any authorised surveillance is legal, necessary and proportionate; and that subject notification, transparency and oversight mechanisms must be defined in legislation. This relatively settled consensus on what constitutes good practice in surveillance law informed the framework for this study. We adopted nine core elements of these three documents as the basis of our analytical framework. We use the shorthand term 'the Principles' to refer to them in this review. The remainder of this section defines and details nine key principles. They are summarised visually in Figure 1.2.

A core principle is the requirement for *prior authorisation of any surveillance* by a **competent judicial authority:** a judge who has responsibility for assessing applications to conduct surveillance against a series of legal tests that are defined in the legislation, and which are designed to protect citizens' constitutional right to privacy. A competent judicial authority is a judge with specific expertise in digital technologies and human rights who has been provided with the appropriate level of resources necessary to assess the volume of applications received from investigating agencies.

The **legality** of each instance of surveillance is a key concern of the Principles. A judge should only be able to authorise surveillance as explicitly defined and allowed for in legislation. Only investigating agencies specifically named in the legislation can be granted authority by the judge. Surveillance legislation should state that any other surveillance is criminal, with the resulting evidence being inadmissible in court, and detail the legal penalties for illegitimate surveillance.

Critically, legislation must define in law what qualifies as a **legitimate aim** of surveillance (e.g. prevention of terrorism). The judge will need to test each surveillance application to determine whether the application addresses a legitimate aim of surveillance as defined in legislation. The precise parameters of 'terrorism', 'national security' and other legitimate aims of surveillance must be defined in law. For privacy rights to be adequately protected, any state surveillance must be narrowly targeted. To achieve this, it is necessary for a limited number of legitimate aims of surveillance to be specified in the legislation (and for all other surveillance to be ruled

illegitimate). Examples of legitimate aims could be national security, terrorism or serious crime. However, it is essential that any such categories are closely specified in legislation in order to enable consistency of application and to prevent abuse of powers. The UN High Commissioner for Human Rights (UNHCHR 2018b: 10) has argued that 'Vague and overbroad justifications, such as unspecific references to 'national security' do not qualify as adequately clear laws'. The definition of what constitutes national security should be sufficiently precise such that it would be consistently interpreted in the same way by any judge.

Assessing legitimate aims is only the first of a series of tests that must be made by the competent judicial authority. The judge must also determine whether there are **sufficient grounds** (i.e. whether there is a high probability that the subject of surveillance presents an imminent threat to a legitimate aim and that the proposed surveillance will produce evidence adequate to removing the threat).

The judge must also assess whether the proposed scope and time frame of surveillance are **necessary and proportionate** to the legitimate aim. The judge must test whether the proposed surveillance is strictly necessary to obtain the information needed (i.e. all other methods having been exhausted or that this method is the least intrusive to privacy) and that it is proportionate in scope and duration to the legitimate aim (UN 2016). The person or premises to be surveilled should be named in the application and the surveillance must be limited to that subject.

To ensure that due process is possible for those who are subjected to surveillance, **notification** should be provided that their privacy was violated, at the earliest appropriate time, to make possible legal appeal, remedy or redress. Annual **transparency** reports should be made public, documenting the number of surveillance requests, grounds and authorisations, to enable public confidence in and accountability of the judicial process and public officials.

The whole process should be overseen by an **independent oversight body** that is independent of the investigating agencies, judiciary and executive, and whose duties and power should be defined in law. The independent oversight body should have access to all applications and authorisations and must be adequately staffed and resourced to carry out its duties.

5. Country report summaries

The next section of this review provides two-page summaries of each of the six country reports that are included in full later in this publication. The intention here is only to provide an accessible visual summary of the detailed and fully referenced reports that follow this introductory synthesis.

Egypt summary

Despite constitutional guarantees of private communications, the protections provided by Egyptian domestic law are among the weakest of the countries in this study. There are few safeguards built into Egyptian law and offences such as offending 'public morality' are nowhere defined in law. There is no transparency or independent oversight mechanism.

The Egyptian government has made extensive use of emergency powers that evade the few protections that do exist. The lack of a single surveillance law, weak definitions regarding the legitimate aims of surveillance and protections, and the absence of safeguards, transparency or oversight mechanisms leave ample opportunity for abuse of surveillance powers.

The large power imbalance between the state and organs of civil society makes it difficult to address existing impunity for state violation of privacy rights. Surveillance law and practice have not been challenged in court. As the Egyptian government continues to increase its surveillance technology capacity, there is a need to strengthen legal protections and practical mechanisms of recourse and remedy.

Recommendations

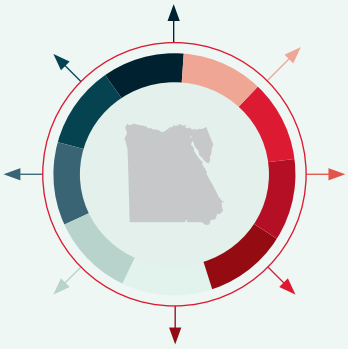
- Incorporate the International Principles into a dedicated surveillance law.
- Create an independent oversight body and publish transparency reports.
- Raise public awareness of privacy and surveillance issues and build the capacity of lawyers and civil society organisations to create a movement for change.
- Use parliamentary oversight powers to review privacy/surveillance and propose changes.
- Use Universal Periodic Review and shadow reports to build pressure for reform.

Egypt principles

Competent judicial authority: Egyptian law does not require prior court authorisation for surveillance. The Anti-Terrorism Law gives the power to public prosecutors or 'any other investigation authority' to conduct surveillance.

Legality: use of imprecise terms, like national security, provides investigating authorities with wide scope for surveillance and few safeguards.

Legitimate aim: Egyptian law considers national security, national emergencies, prevention of terrorism and cybercrimes to be legitimate aims of surveillance. What constitutes 'national security' is very broadly defined as 'everything related to the independence, stability, and security of the homeland and anything related to the affairs of the Presidency, the Ministry



of Defence and General Intelligence, and the Administrative Oversight Authority'.

Reasonable grounds: the Egyptian legal framework does not require any test for reasonable suspicion prior to authorising surveillance.

Necessity: Egyptian law does not require a test of necessity.

Proportionality: there is no clarity in Egyptian law as to what a proportionality test should encompass.

Notification: there is no right to subject notification in Egypt.

Transparency: there is no public reporting requirement.

Independent oversight: there is no independent oversight body in Egypt, making the state the sole judge, jury and regulator.

Kenya summary

Kenya's compulsory biometric citizen ID system, *huduma namba*, alongside mandatory mobile phone registration, combined with state monitoring of citizen's internet, mobile and financial activity, provides the most comprehensive state surveillance infrastructure of the six countries studied.

Privacy rights that are guaranteed in the constitution and domestic laws have been violated by state surveillance practices. As several court cases have shown, surveillance powers justified with reference to preventing terrorism can be used to enable mass surveillance of other groups. Kenya does not have a specific surveillance law as is the case in South Africa and Nigeria. Instead, a multiplicity of laws regulate surveillance, and it is not always clear which law applies.

Kenya has a strong civil society, and independent media and courts. Strategic legislation has been used successfully to raise public awareness about privacy violations and surveillance practices and has led to legal reform.

Recommendations

- Incorporate the International Principles into a single surveillance law.
- Initiate annual transparency reports of surveillance applications and authorisations.
- Create an independent oversight body with sufficient resources.
- Raise public awareness about privacy rights and surveillance practices to mobilise political will to improve legislation and practice.

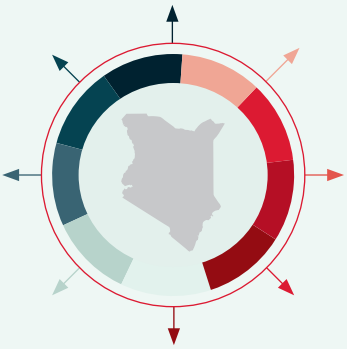
Kenya principles

Competent judicial authority: Kenyan law requires prior authorisation of surveillance from a judge who must test applications against criteria of legality, necessity and proportionality.

Legality: a multiplicity of relevant laws create uncertainty about legal surveillance powers and although case law is clarifying, a single surveillance law would be beneficial.

Legitimate aim: national security is the only legally defined legitimate aim for surveillance in Kenya; however, the definition of national security is very broad.

Reasonable grounds: there is no explicit requirement to show evidence that the proposed surveillance subject has or is about to threaten national security.



Necessity: applications to conduct surveillance must show necessity, but how necessity must be tested is not defined.

Proportionality: different laws pay varying attention to proportionality and it can be unclear which law is being relied upon. The absence of reporting or oversight mechanisms make it impossible to assess whether proportionality is being tested. A single surveillance law with defined mechanisms is needed.

Notification: there is no right to subject notification in Kenya.

Transparency: there is no requirement for public reporting in Kenya.

Independent oversight: there is no independent oversight body in Kenya.

Nigeria summary

Nigeria spends the most on surveillance technologies of any country included in this study, with reported totals in the order of hundreds of millions of dollars. Digital surveillance tools have been procured from Israel, Germany, the UK, US and China. There are multiple examples of state surveillance that are neither legal, necessary nor proportionate, including on journalists, peaceful activists and opposition politicians.

These infringements have yet to be challenged in court. New investments are now being made in biometric ID, CCTV and licence plate surveillance. Civil rights organisations in Nigeria are concerned about use of illegitimate surveillance and are worried that mass surveillance is becoming normalised. The 2019 Lawful Interception of Communications Regulation (LICR) is the Nigerian law that most directly defines the surveillance powers of the state, but other powers are also provided in an array of other laws.

There are clear opportunities to improve surveillance law in Nigeria by tightening up legal definitions and introducing notifications, transparency and independent oversight. If impunity for illegitimate surveillance is to end, there is a need to raise awareness among the public, media and civil society to bring about revision of the law and practice until all surveillance is narrowly targeted, legal and necessary to secure a legitimate aim.

Recommendations

- Incorporate all of the African Declaration and International Principles into a revised LICR that takes precedence over all preceding Nigerian law.
- Annual transparency reports should be made public.
- An independent oversight body should be established.
- Civil society and media should raise awareness about privacy rights and mobilise the necessary political to end impunity for violations of constitutional privacy rights.

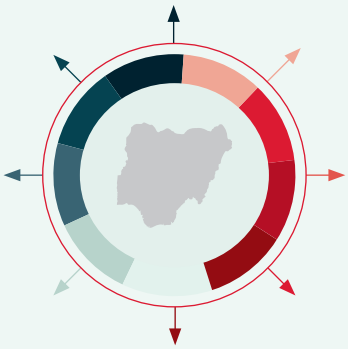
Nigeria principles

Competent judicial authority: Nigerian law requires prior authorisation of surveillance by a judge, although exceptions apply in emergencies.

Legality: Nigerian law requires that any restriction to the right of privacy be defined in law. The LICR authorises only the Department of State Security, the Nigeria Police Force and the Office of the National Security Adviser to conduct surveillance yet other agencies are procuring surveillance technologies.

Legitimate aim: the LICR specifies five legitimate aims of surveillance; however, what qualifies as national security. is not defined in law, providing scope for inconsistency or abuse of power

Reasonable grounds: in order to justify surveillance, Nigerian law requires a judge to test that 'facts alleged in the application



are reasonable and persuasive enough' to constitute a threat to a legitimate aim.

Necessity: the LICR requires necessity to authorise surveillance, but Nigerian police often detain journalists and surveil the contents of their phone without warrants and with impunity.

Proportionality: the LICR requires a detailed description of the target and duration of proposed surveillance, but a test of proportionality is not included in the law.

Notification: there is no requirement in Nigerian law for subject notification.

Transparency: annual reports are made to the attorney general but not to the public, so it is not possible for citizens or legislators to know whether the legislation is working as intended.

Independent oversight: there is no requirement in Nigerian law for an independent oversight mechanism.

Senegal summary

Senegal enjoys a stable democracy and the right to privacy of communications is an inviolable constitutional right. National security concerns have been used to justify expanded surveillance powers. The state has made mobile phone registration mandatory and has purchased FinSpy mobile phone surveillance technology.

Senegal has made the second-highest surveillance data requests of any country according to the transparency report of mobile telecommunications company Orange. The 2016 Intelligence Services Law documents the circumstances in which the state gives itself the power to violate privacy. This aligns with the recommendation of the International Principles that any surveillance that violates privacy rights must be legal, necessary and proportionate.

There are opportunities to improve the legal framework for surveillance as there are presently no transparency reporting, independent oversight or subject notification mechanisms. There has been no documented legal case challenging state surveillance processes. This may be due in part to the secret nature of surveillance and the absence of any transparency reporting. The African Declaration and International Principles could help improve privacy safeguards and independent oversight.

Recommendations

- Public transparency reports and independent oversight would increase trust in the system.
- Key terms, such as national security, should be defined in law and anchored in human rights.
- Restrictions on encryption should be removed to protect the right to anonymity.
- Further research is necessary on the surveillance taking place and any impact on human rights.
- Public awareness about citizens' privacy rights and surveillance help guard against overreach.

Senegal principles

Competent judicial authority: prior authorisation of an investigating judge is required to conduct surveillance under the Code of Criminal Procedure.

Legality: the Intelligence Services Law stipulates that intelligence agents must only act in accordance with legislation.

Legitimate aim: the law defines a limited number of 'legitimate aims' for surveillance including preventing terrorist attack. However, the Cybercrime Law allows surveillance for prevention of crimes more widely.

Reasonable grounds: investigating authorities are able to conduct surveillance if there is presumption of a crime, but the law does not define what constitutes reasonable grounds.

Necessity: the Intelligence Services Law and Code of

Criminal Procedure, determine that surveillance measures can only be adopted if it is the only means to access the information. There is insufficient clarity in law about how necessity must be shown and tested.

Proportionality: the Intelligence Services Law states that surveillance must be proportionate to the seriousness of the threat. This assessment is carried out by the public prosecutor.

Notification: there is no right to subject notification in Senegalese surveillance law.

Transparency: there is no legal requirement for public reporting of the number and type of surveillance requests and authorisations, reducing public accountability.

Independent oversight: there is no independent oversight body to provide confidence that the law is being implemented as legislators intended and is consistent with constitutional rights.

South Africa summary

South Africa has a clear surveillance law framework and sufficient civil society capacity to mount strategic litigation, resulting in the most tractable surveillance law framework of the six countries studied. The South African state has abused its surveillance powers but has been held accountable by civil society and the court has suspended the state's surveillance powers.

South Africa has the advantage of a dedicated surveillance law. Implemented in the wake of 9/11 to enable surveillance to prevent terrorist threats, in practice the majority of surveillance authorisations are for a wide range of other crimes. South Africa does not face the scale of terrorist threats encountered elsewhere yet has among the most advanced surveillance capabilities.

The state has been found guilty of using surveillance outside of the law. State surveillance powers have been used to monitor political opposition and business competitors. A challenge in the Constitutional Court found the state guilty of carrying out unlawful mass surveillance and foreign signal interception. Civil society has raised concerns about the rapid expansion of surveillance infrastructure including biometric registration, mandatory SIM registration, and CCTV surveillance.

Recommendations

- A genuinely independent oversight body is needed that is dedicated to surveillance.
- Legal precision of terms such as national security is needed to ensure consistent implementation.
- More work is needed to raise public awareness of privacy rights and surveillance practices.
- An urgent legal rights assessment is needed of facial recognition surveillance in South Africa.
- Further research is necessary on surveillance actors, tools, incidence and remedies.

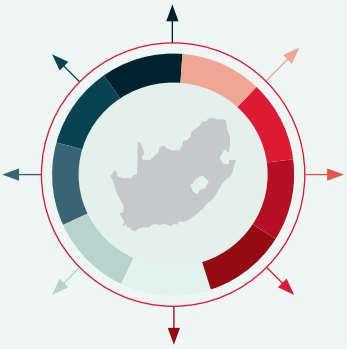
South Africa principles

Competent judicial authority: prior authorisation is required. The constitutional court ruled in the amaBhungane case that the judge was insufficiently independent, and insufficiently resourced, to adequately test the high level of surveillance requests.

Legality: the constitutional court suspended RICA powers to authorise surveillance, after ruling that state surveillance practice went beyond what was permitted in law.

Legitimate aim: legitimate aims include serious offences, public health or safety, national security or compelling national economic interests. These overly broad categories have been used to target legal peaceful journalists and activists.

Reasonable grounds: proof of reasonable grounds is required to the satisfaction of the judge, prior to authorisation of surveillance. However, the ability of the judge to adequately assess proof of reasonable



grounds is currently compromised due to under-resourcing.

Necessity: necessity is required. In the amaBhungane case the court ruled that the bulk surveillance carried out by the state exceeded that necessary to secure a legitimate aim. .

Proportionality: proportionality is required. The same court ruled that the mass surveillance being practised in South Africa was disproportionate to the threat.

Notification: there was no legal right to subject notification in RICA, but in 2021 the Constitutional Court ruled that notifications should be made to allow due process.

Transparency: transparency reporting is required by the RICA judge to a parliamentary committee, but the level of detail is insufficient to fully inform or enable effective oversight.

Independent oversight: although oversight is provided by the Inspector-General of Intelligence and a parliamentary committee, there is no oversight body that is independent of the RICA judge and state agencies, as recommended in the UN Draft Instrument.

Sudan summary

In Sudan, the right to privacy is protected by the constitution, through international conventions and in domestic law. However, the legal safeguards and protections in Sudan's surveillance law framework are among the worst of the countries studied.

This is perhaps a legacy of a long period under oppressive rule. Prior to the 2018 revolution, Sudanese government surveillance targeted activists, lawyers and journalists by intercepting electronic messages between private citizens. Omar Al Bashir's regime included a special unit called the 'Cyber-Jihadists' to spy on government critics, human rights activists, journalists and opposition parties. Sudan is known to use software company Hacking Team's spyware for this purpose.

The new government continues to rely on foreign software to spy on citizens and has used the Covid-19 pandemic as an opportunity to introduce new surveillance technologies and limit people's digital rights. There are many opportunities for the government to improve legislation and practice in line with the Cairo Declaration on Human Rights in Islam (1990) and the African Declaration (2019).

Recommendations

- Define the legitimate aims of surveillance in law.
- Require prior authorisation from an independent judge for all surveillance.
- Require judges to test requests for reasonable grounds, legality, necessity and proportionality.
- Raise public awareness of privacy rights and build civil society capacity to challenge law.
- Use human rights law as a basis for legal review and revision of legislation.
- Conduct research into the experiences of other countries to guide Sudanese practice.

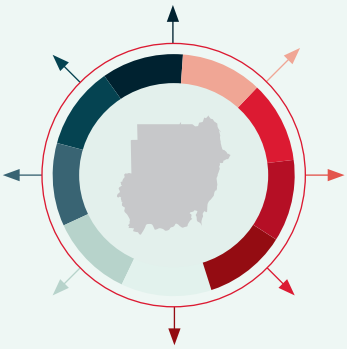
Sudan principles

Competent judicial authority: although other Sudanese laws require prior judicial authorisation for surveillance, the National Security Law gives national security officers the power to seize any information or communication data without judicial authority.

Legality: surveillance should only be carried out as authorised in law, but Sudanese law lacks legal precision, providing opportunity for abuse of power.

Legitimate aim: the Cybercrimes Law does not specify the legitimate aims of surveillance. Laws refer to policing 'moral and public order', but these terms are nowhere defined in law, creating scope for abuse and inconsistency of application.

Reasonable grounds: there is no legal requirement to show



reasonable grounds prior to conducting surveillance in Sudan.

Necessity: there is no legal requirement to show that surveillance is necessary prior to authorisation in Sudan.

Proportionality: there is no legal requirement to show that proposed surveillance is proportionate to the perceived threat.

Notification: there is no legal right to subject notification in Sudan.

Transparency: there is no legal requirement to publish transparency reports of surveillance applications and authorisations in Sudan.

Independent oversight: there is no independent surveillance oversight body in Sudan to provide confidence that the law is being applied consistently within constitutional rights.

Figure 1.3 provides a visual summary of the provisions of surveillance law in each country studied. This table is derived from the more comprehensive analysis contained in each of the full country reports included in this publication. Each of the full country reports contains sections addressing a specific area of privacy rights and that country's surveillance law framework.

Figure 1.3 Privacy Protections Provided in Surveillance Legislation

	EG*	KE	NG	SG	SA**	SD***
Competent judicial authority: a judge knowledgeable in digital technologies and human rights to assess and authorise requests to conduct surveillance from investigating agencies of the state.	◒	◒	●	●	●	◒
Legality: surveillance carried out only within parameters and by agencies specified in the legislation. The legislation criminalises all other surveillance and specifies penalties.	◒	◒	●	●	●	◒
Legitimate aim: law closely defines the only legitimate aims of surveillance e.g. prevention of terrorism or serious crime with a legal punishment of 10 or more years in jail.	◒	◒	●	●	●	◒
Reasonable grounds: judge must test whether there is a high degree of threat and a high probability that surveillance will produce evidence that removes the threat to a legitimate aim.	◒	●	●	●	●	◒
Necessary: judge must test whether surveillance is necessary to secure the evidence and that no other less invasive method is available to address legitimate aim.	◒	◒	●	●	●	○
Proportionality: judge must test whether proposed surveillance is limited in scope, and that the duration is in proportion to the evidence needed to remove the threat.	◒	◒	●	●	●	◒
Notification: at the earliest appropriate time the subject of surveillance should be notified of the occurrence to provide opportunity for legal appeal and due process.	○	○	○	○	○	○
Transparency: annual transparency reports should publicise number of requests, grounds, and authorisations to enable public accountability of process and public officials.	○	○	○	○	●	○
Independent oversight: public oversight mechanisms should be established to ensure transparency and accountability of surveillance practices.	○	○	○	○	●	○

* Although Egyptian law provides some partial protections the Emergency Law in place since 2017 removes all of these protections

** South Africa's RICA law provides most protections but parts of the law have been suspended by the constitutional court to add new protections

*** Although some protections are provided in Sudanese law the current National Securty law enables state agencies to override the protections

KEY

- ● Provided in legislation
- ◒ Partial provision
- ○ No provision in legislation

6. Findings

This section presents our main findings regarding the existing frameworks for African surveillance law when reviewed against the criteria contained in the Principles.

A positive finding is that the right to privacy is guaranteed in each country in three ways: in the constitution, in international conventions and in domestic laws. In all six countries, the fundamental human right to privacy of communication and correspondence is explicitly guaranteed in each country's constitution. In all six cases, the country has also adopted international conventions that further protect privacy rights, including the Universal Declaration of Human Rights (UN 1948), the International Covenant on Civil and Political Rights (UN 1966) and the Declaration of Principles of Freedom of Expression and Access to Information in Africa (African Commission 2019). And in each case these constitutional and conventional rights to privacy are additionally guaranteed in domestic legislation – most often reaffirmed in several different laws. As the Nigeria and Egypt country reports illustrate, it is not uncommon for a country to be party to six or seven international conventions or declarations securing privacy rights for its citizens, in addition to making privacy rights explicit in the constitution and national laws (Oloyede this edited collection; Farahat this edited collection). Although African constitutions 'guarantee' or make 'inviolable' privacy rights, domestic laws create exceptions where state agencies can legally carry out surveillance.

Governments are using new domestic laws to award themselves increasing surveillance powers that violate privacy rights. A wide range of justifications are given to the public for needing these new powers, from the threat of terrorist attack to economic interests and protecting public morality. In Kenya alone, arguments deployed by the government to expand surveillance have included: national security, money-laundering, monitoring state officials, control of hate speech, public health, fake news, and protecting intellectual property rights (Mutung'u this edited collection). Playing the 'national security' card is often sufficient, as it trumps protecting privacy rights by framing the decision as a binary choice between the interests of all good citizens and those of a few suspected of serious crimes. However, evidence in this report demonstrates that surveillance powers obtained to narrowly target terrorists are used to spy on peaceful activists, journalists, business competitors, political rivals and governments. Civil society organisations are concerned that governments are building their capacity for mass

surveillance and normalising surveillance (Mutung'u this edited collection; Oloyede this edited collection).

Surveillance powers intended to narrowly target the most serious crimes are used widely. There is ample evidence of state surveillance powers being used to violate the privacy rights of citizens who have no links to terrorism and who present no conceivable threat to legitimate aims. The South Africa report provides evidence of state surveillance being used illegally for business surveillance, targeting journalists and civil society organisations (Mutung'u this edited collection). The Sudan report shows that state surveillance has been used to target peaceful critics of the government, lawyers, and journalists (Farahat this edited collection). In Kenya, civil society organisations have criticised the government for extra-legal surveillance of human rights defenders, minors and people living with HIV (Mutung'u this edited collection). According to the transparency report of mobile telecommunications company Orange, Senegal made the second-highest number of surveillance requests of any country using their service (Oloyede this edited collection).

In all six countries studied, there is insufficient clarity about what surveillance is legal. Legal imprecision is a significant problem in existing surveillance law frameworks, including as explained in the Egypt country report (Farahat this edited collection). What is considered to be a matter of national security or national interest is insufficiently well defined in law, making it impossible to apply consistently, providing scope for abuse of power and making legal challenges practically impossible. This lack of clear definition may be by design or omission, but in either case greater legal precision is in the interests of privacy rights. In cases such as Sudan (Farahat this edited collection) it is the absence of clarity about what qualifies as the legitimate aims of surveillance that is the root of the problem. In other countries, such as South Africa, the absence of clear legal definitions has created opportunities for inconsistency of application or abuse of powers (Mutung'u this edited collection). In some countries, such as Kenya and Senegal, the lack of legal clarity is due to confusion caused by a multiplicity of laws prescribing surveillance powers (Mutung'u this edited collection; Oloyede this edited collection). There are opportunities to improve the definition of the legitimate aims of surveillance in all of the countries included in this study.

In all six countries studied, impunity exists for those carrying out illegal surveillance. Evidence was found of surveillance outside of that permitted in law; however, no evidence was found of any prosecutions or disciplinary action taken against investigating agencies acting illegally. Surveillance should only occur as prescribed in legislation. All other surveillance is by definition illegitimate and should incur penalties that should be detailed in

legislation. Legal clarity about (il)legitimate surveillance is essential to foster public understanding, enable consistent application and avoid abuse of powers. Surveillance legislation needs to be clear about which agencies can conduct surveillance; who can judge requests to conduct surveillance; what legal tests a judge must apply to requests; and what legal penalties apply for illegitimate surveillance. The International Principles, UN Draft Legal Instrument and African Declaration are useful resources for improving legal precision regarding surveillance.

The tests of necessity and proportionality are insufficient in all six countries. It is widely accepted in international law that any limitation of fundamental human rights must be 'legal, necessary and proportionate'. However, all of the country reports draw attention to the need to either provide clearer definition of the terms necessity and proportionality or the mechanisms by which they are assessed. The legislation in Egypt and Sudan does not require any tests of necessity or proportionality (Farahat this edited collection). In Senegal and Nigeria, the tests are required but the testing mechanisms are insufficiently detailed (Oloyede this edited collection). In Kenya and South Africa, where the law is clear, evidence exists that surveillance has taken place in cases where it was neither necessary nor proportionate (Mutung'u this edited collection). The African Declaration is a useful resource for definitions of necessity and proportionality (African Commission 2019) and the International Principles and UN Draft Legal Instrument are helpful regarding assessment mechanisms (EFF 2014; UNHCHR 2018a).

Additional safeguards, transparency and independent oversight are required in all six countries. Recommendations from the six country reports focus on three clear gaps in existing frameworks: judicial tests of surveillance applications, transparency reporting and independent oversight. The most important safeguarding mechanism is a judge who is technically competent and sufficiently well-resourced to assess all surveillance requests against legitimate aims, reasonable grounds, legality, necessity and proportionality. All governments (and mobile and internet service providers) should also publish annual transparency reports of surveillance requests and authorisations. The third measure is the establishment of a dedicated independent oversight body to improve public accountability and boost confidence that the law is being consistently applied to protect national interests rather than private economic or partisan political interests. . South Africa has the best safeguards of the countries studied, although the Constitutional Court ruled that the authorising judge had insufficient resources to adequately assess the very high volume of surveillance applications received. The Court also found that the level of detail contained in the transparency reports was insufficient to enable effective oversight.

In all six countries studied, existing surveillance legislation and practice fall short of the Principles detailed in the African Declaration, UN Draft Legal Instrument and International Principles. There is an urgent need to improve privacy protections and end impunity for illegitimate surveillance. The Principles provide a clear actionable basis to enable narrowly targeted surveillance within a framework that provides appropriate protections for privacy rights. The use of the International Principles avoids centring practice from the global North and instead relies on widely supported principles that reflect human right conventions that already form part of African countries' existing constitutional and legal frameworks.

There appears to be an advantage in having a single surveillance law. In the Senegal and Kenya country reports, it was noted that confusion is caused by a multitude of different laws that provide surveillance powers (Oloyede this edited collection; Mutung'u this *edited collection*). The result is that it may not always be clear from which piece of legislation an investigating authority derives its authority. In Nigeria, it is not yet clear whether the new LICR will clarify this situation (LICR 2019). Where there is a single piece of legislation that supersedes prior legislation and provides legal precision, the opportunity for inconsistency of application or abuse of powers is reduced. In South Africa, RICA is not perfect but having a dedicated piece of legislation has provided a central focus for efforts to establish the balance between privacy rights and legal surveillance, including an unambiguous target for efforts to reform and improve the law over time (Mutung'u this edited collection).

Existing surveillance law is failing to protect privacy in all six countries. Despite good privacy protection from national constitutions, international conventions and in national laws, in all of the countries studied surveillance is expanding and privacy rights are being eroded. States are rapidly expanding investments in surveillance technologies and enacting new laws that provide them with new surveillance powers. The capacity for expanding surveillance is being built both in countries with significant national security threats and in countries where there are none. South Africa does not have national security threats in the way that Kenya has, but it has been conducting bulk surveillance in ways that its courts ruled were not legal, necessary or proportionate (Mutung'u this edited collection).

Strategic litigation can improve surveillance law and practice in some African countries. The reports from South Africa and Kenya have shown that legal challenges can be fruitful in raising public awareness and securing reforms, partly due to the strong constitutional protection of privacy rights in those countries (Mutung'u this edited collection). Although surveillance law or practice have not yet been challenged in the other countries studied,

the report authors note that constitutional courts have proven fruitful in other areas and that parliamentary committees and review processes offer additional options to leverage privacy guaranteed by national constitutions, international conventions and national law (Farahat this edited collection).

However, legislative reform alone is insufficient to deliver privacy rights. The country reports provide ample evidence that governments conduct illegitimate surveillance outside of what is allowed for in law. This has been evidenced in the Cambridge Analytica scandal in Nigeria and Kenya, by the Snowden revelations about South Africa and most recently by investigations of states using NSO Group's Pegasus Spyware to spy on peaceful activists, journalists and political opponents (Ekdale and Tully 2020; Snowden 2015; Amnesty 2021).

The evidence is that governments are circumventing the law, violating citizens' rights and conducting illegitimate surveillance. The power imbalance between citizens and the state is a factor in citizens' ability to hold governments accountable to the law. South Africa's strong civil society, independent courts and media freedoms make the legal framework for surveillance more tractable than in the other countries studied. This is evidenced in the recent legal challenge that resulted in the suspension of surveillance powers in order to reform them (Mutung'u this edited collection).

Improving the surveillance law framework requires mobilising the political will for reform. The framework for surveillance law appears to be more open to challenge where civil society actors have the ability to hold governments accountable to their commitments to protect privacy rights that are enshrined in constitutional, international and domestic laws. Sufficient guidance already exists on how to draft excellent surveillance laws (EFF 2014; UNHCHR 2018a; African Commission 2019). What is lacking in many countries is the political will for legislative reform in this direction and capacity in civil society to hold governments accountable to the spirit and letter of the law. Like the other countries in this study, South Africa's surveillance law is imperfect; its government has been conducting illegal surveillance on citizens, and it is increasing its legal and technological capacity to further expand surveillance. However, South Africa, as well as Kenya, have sufficient capacity in civil society to identify problems and work in collaboration with constitutional lawyers and journalists to press successfully for reform of surveillance legislation and practice.

It may be that strategic litigation to challenge the law and its application will prove useful in raising awareness and creating legal precision. The South Africa country report (Mutung'u this edited collection) provides an example of legal challenges being used to produce court rulings that raised public awareness, clarified the law and introduced new privacy

safeguards. The Kenya country report (Mutung'u this edited collection) illustrates how internet or mobile service providers can challenge in court government requirements to store customers' communication records and make them available to security agencies. It can be argued in court that any bulk interception contravenes constitutional guarantees of privacy of communications as well as the 'necessary and proportionate' tests derived from international law. In these cases strategic litigation has gained substantial media coverage, raised public awareness and strengthened the capacity of civil society to hold governments accountable in law. The situation is arguably more tractable in South Africa and Kenya than other countries, but the country report from Egypt (Farahat this edited collection) argues that precedents in that country suggest this avenue may also be possible in other countries.

7. Conclusion

This research provides the first comparative analysis of African legal surveillance frameworks. It set out to understand what legal provisions currently exist to protect privacy and enable targeted surveillance in six African countries: Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan. The objective was to understand existing strengths, identify opportunities for improvement and produce actionable recommendations. We used nine core elements from existing international guidance on surveillance law as a framework for our analysis. This section draws together some conclusions before presenting recommendations for policy, practice and further research.

This review found that surveillance practice is eroding privacy rights due to six factors:

1. The introduction of new laws that expand state surveillance powers.
2. Lack of legal precision and privacy safeguards in existing surveillance legislation.
3. Increased supply of new surveillance technologies that enable illegitimate surveillance.
4. State agencies regularly conducting surveillance outside of what is permitted in law.
5. Impunity for those committing illegitimate acts of surveillance.
6. Insufficient capacity in civil society to hold the state fully accountable in law.

The report argues that citizens have good reason to value privacy. The right to communicate free from state surveillance is an intrinsically valuable freedom. It also has instrumental value for democracy. People who experience repression may need to communicate in private to build movement for change. Surveillance violates privacy rights. Its covert nature and the large power imbalance between states and citizens make it important to provide strong privacy protections in surveillance laws. These protections include prior authorisation by a competent judicial authority which should assess surveillance applications against tests for legality, legitimate aims, reasonable grounds, necessity and proportionality. Surveillance law should also require safeguards including subject notification, transparency reporting and independent oversight.

Privacy rights are well established legally but increasingly violated by state surveillance. In all six countries the right to private communication is explicitly guaranteed in the national constitution, international conventions, and

domestic laws. However, these privacy rights are increasingly being violated by a rapid expansion of state surveillance practices. The country reports noted increased state investments in mobile spyware, artificial intelligence-based internet surveillance, surveillance cameras, licence plate recognition and facial recognition; the introduction of compulsory biometric ID systems and mandatory mobile SIM card registration laws; and the compulsory retention of data by mobile, internet and banking companies for access by state security agencies. The country reports provide evidence that much of this increased surveillance is illegitimate in its aims and exceeds what is legal, necessary and proportionate. There is insufficient documentation about which companies from the global North, are providing which states in the global South, with which surveillance technologies, and with what outcomes. This report is one of the first attempts to document this expansion of surveillance technologies across Africa, but is modest in its scope. Further research is needed if efforts to mitigate and curtail illegitimate surveillance are to be well targeted and successful.

States are awarding themselves ever-greater surveillance powers that violate privacy rights. In every country we studied, the state used threats to national security to justify expansion of its surveillance powers. National security was often a Trojan horse to establish surveillance powers which were then deployed for other purposes. Each of the six country reports begins by reflecting on the reasons given by African governments for awarding themselves new powers of surveillance. The reasons provided to the public and lawmakers were often not consistent with the application of the powers once attained. All governments used terrorism or the need to provide national security as a key motive for extending state surveillance powers. This was the case both in countries that had clear terrorist threats to national security and in countries that had none. The six country reports provide evidence that the application of surveillance powers once obtained was not confined to legitimate national security interests but in practice was used to further partisan political and private business interests, as well as for mass surveillance and general policing. These are illegitimate aims of surveillance and contravene the letter and spirit of human rights law.

State violation of citizens' privacy involves both legal and illegal surveillance practices. States are passing new laws to award themselves increased surveillance powers. They argue that these new surveillance powers are necessary to protect citizens from terrorist threats and to secure national security and national interests. The absence of a legal definition of these legal aims of surveillance has led to the surveillance of many journalists, opposition politicians and peaceful activists in ways that remove freedoms and threaten democracy and social justice. The study shows that the state is expanding its surveillance capabilities both in countries such

as Kenya, which have a genuine terrorist threat, and South Africa, where there is no comparable threat. The study also shows that once surveillance powers exist, they are most often used on non-terrorist subjects including spying on political opponents and business rivals. Civil society organisations are worried that, rather than restricting itself to narrowly targeted legitimate surveillance, states are increasingly conducting mass surveillance and illegitimate surveillance of those who oppose their private or partisan interests. There is a concern that surveillance creep is taking place, that mass surveillance is becoming normalised and privacy rights eroded, and that illegitimate surveillance is being conducted with impunity.

There are clear opportunities to improve existing surveillance law frameworks in all six countries. A single, dedicated surveillance law is preferable to multiple laws defining surveillance powers. Laws in all six countries can be improved by incorporating the International Principles. Specific attention needs to be spent closely defining legitimate aims and prior authorisation tests. Safeguards, transparency reporting and independent oversight needs strengthening in all six countries. The African Declaration, UN Draft Legal Instrument and International Principles are helpful in these regards.

Legislation alone is insufficient. States conduct illegitimate surveillance in both democratic and authoritarian countries. Holding states accountable to the law and the ability to exercise, defend and expand fundamental rights require open civic space and an independent civil society, media and judiciary. Political will must also be mobilised if legal reform and state accountability to the law are to be achieved. The pathways to reform will be very different in different countries. Where civic space exists, civil society is relatively strong and courts and media independent, the situation may prove to be more tractable for reform of laws and surveillance practices. Where civic space is restricted or closed, civil society relatively weak, and courts and media are partisan, the situation may seem intractable and alternative approaches will be necessary that are cognisant of safeguarding issues. Contextual situational analyses will be necessary to define appropriate action in each country.

It is necessary to build public awareness about privacy rights and surveillance practices and to build civil society capacity to bring about change. This will require coordinated activity involving citizens, lawyers, journalists, activists, researchers and policymakers. Different programmes of action will be appropriate in different countries. The pathways to change are likely to be different in Egypt and Sudan when compared to Kenya and South Africa due to substantially different political contexts, civic space and levels of independence in the media, judiciary and civil society. Applied

research with activists, journalists and lawyers should include situational and stakeholder analyses to inform theories of change and action.

Strategic litigation may be one effective way to improve legislation and build capacity. Challenging the legality of surveillance law in Kenya and South Africa in the constitutional courts has been a productive way of raising public awareness, expanding citizen engagement and building civil society capacity to mobilise movement for change. The country report author for Egypt and Sudan suggested this may be productive, despite the less tractable situation. Parliamentary committees, judicial review processes and other established mechanisms may also be pathways to change.

There is a danger that in the absence of countervailing pressure from civil society, political, economic and technological factors will lead to surveillance-creep, the normalisation of mass surveillance and a descent into digital authoritarianism. This is not inevitable. It is possible to balance the need for narrowly targeted surveillance of the most serious crimes with the privacy rights of citizens. The UN General Assembly urges states:

> while countering terrorism… to safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means.
> (UN 2017)

Recommendations

Arising from this analysis of the surveillance law frameworks in six African countries, the following recommendations emerge for policy, practice and further research:

- Governments should draft a single, dedicated surveillance law that supersedes previous legislation, reasserts privacy rights and closely defines the legitimate aims of surveillance.
- Governments should incorporate the International Principles into surveillance law.
- Governments should end impunity for illegal surveillance by defining in law the penalties for illegitimate surveillance and enforce them consistently.
- The supply of surveillance technologies to countries that violate privacy rights should be ended.
- Civil society organisations should generate public awareness about privacy rights and surveillance practices and hold state and non-state actors accountable to the law.
- Civil society organisations should create pressure to mobilise the political will for legal reform by forging a coalition of human rights activists, journalists, policymakers, technologists and researchers.
- Further research is necessary to provide guidance on what has (not) worked in practice to restrict illegitimate surveillance and improve privacy protections.
- Further research is necessary to map which companies are supplying which surveillance technologies to which states and with what effects in order that efforts to mitigate and curtail illegitimate surveillance are well targeted and successful.
- Further research is necessary to analyse the local drivers, stakeholders and practices of surveillance to plot potential pathways to reform in each country.

Bibliography

ACLU (2021) ***Surveillance Under the PATRIOT Act***, New York: African Civil Liberties Union (accessed 18 September 2021)

African Commission (2019) ***Declaration of Principles of Freedom of Expression and Access to Information in Africa***, Banjul: African Commission on Human and Peoples' Rights (accessed 18 September 2021)

Amnesty International (2021) ***Forensic Methodology Report: How to catch NSO Group's Pegasus***, London: Amnesty International Forensic Laboratory (accessed 18 September 2021)

Article 19 (2019) ***UK: Government should not use coronavirus as cover for expanding surveillance regime***, London: Article 19 (accessed 18 September 2021)

Bernal, P. (2016) **Data gathering, surveillance and human rights: recasting the debate**, *Journal of Cyber Policy Vol 1(2): 243–264* (accessed 18 September 2021)

Bradford Franklin, S. (2019) ***Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records***, New York: Just Security (accessed 18 September 2021)

CIVICUS (2020) ***People Power Under Attack 2020,*** Johannesburg: CIVICUS (accessed 18 September 2021)

Courage Foundation and Transparency Toolkit (2015) ***Snowden Doc Search*** (accessed 18 September 2021)

Crocker, A. (2015) ***Appeals Court Rules NSA Phone Records Dragnet is Illegal***, Electronic Frontier Foundation (accessed 18 September 2021)

Dencik, L. and Cable, J. (2017) Digital Citizenship and Surveillance – The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks, *International Journal of Communication* Vol. XI: 763–781.

Duncan, J. (2018) *Stopping the Spies: constructing and resisting the surveillance state in South Africa,* Johannesburg: Wits University Press.

EFF (2014) ***Necessary and Proportionate: Principles on the Application of Human Rights Law to Communications Surveillance***, Electronic Frontier Foundation (EFF) (accessed 18 September 2021)

EFF (2013) ***International Principles on the Application of Human Rights to Communications Surveillance***, Electronic Frontier Foundation (EFF) (accessed 18 September 2021)

Ekdale, B. and Tully, M. (2020) **African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers**, *Journal of African Journalism Studies* Vol 40(4): 27–43 (accessed 18 September 2021)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Carnegie Endowment for International Peace (accessed 18 September 2021)

Freedom House (2021) ***Democracy Under Siege***, Washington DC: Freedom House (accessed 18 September 2021)

Freedom House (2018) ***The Rise of Digital Authoritarianism***, Washington DC: Freedom House (accessed 18 September 2021)

Gerhold, L., Bartl, G. and Haake, N. (2017) Security culture 2030. How security experts assess the future state of privatisation, surveillance, security technologies and risk awareness in Germany, *Futures* 87: 50–64

Investigatory Powers Act (2020) ***The Investigatory Powers Act 2016 (Commencement No. 12) Regulations 2020***, UK Statutory Instrument 2020 No. 766 (C. 26), London (accessed 18 September 2021)

Islamic Conference (1990) ***Cairo Declaration on Human Rights in Islam***, World Conf. on Human Rights, 4th Session (accessed 18 September 2021)

Jili, B. (2020) ***Surveillance Technology a Concern for Many in Africa***, New African Daily (accessed 18 September 2021)

Mute, L.M. (2019) ***Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019***, African Commission on Human and Peoples' Rights (accessed 18 September 2021)

OAU (1981) ***African Charter on Human and People's Rights***, Banjul: Organisation of African Unity (accessed 18 September 2021)

Privacy International (2019) ***Guide to International Law and Surveillance*** (accessed 18 September 2021)

Roberts, T. (ed.) (2021) ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries***, Brighton: Institute of Development Studies. DOI: 10.19088/IDS.2021.003 (accessed 18 September 2021)

Roberts, T. and Mohamed Ali, A. (2021) Opening and Closing Online Civic Space in Africa: An Introduction to the Ten Digital Rights Landscape Reports, in T. Roberts (ed.), ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries***, Brighton: Institute of Development Studies. DOI: 10.19088/IDS.2021.005 (accessed 18 September 2021)

UN (2016) ***Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression***, New York: United Nations General Assembly (accessed 18 September 2021)

UN (1966) ***International Covenant on Civil and Political Rights***, New York: United Nations (UN) (accessed 18 September 2021)

UN (1948) ***Universal Declaration of Human Rights***, New York: United Nations (UN) (accessed 18 September 2021)

UNHCHR (2018a) ***Draft Legal Instrument on Government-led Surveillance and Privacy***, Geneva: United Nations Office of the High Commissioner on Human Rights (accessed 18 September 2021)

UNHCHR (2018b) ***Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age***, UN Doc. A/HRC/39/29 (3 August 2018), Geneva: United Nations Office of the High Commissioner on Human Rights (accessed 18 September 2021)

UNHRC (2018) ***The Right to Privacy in the Digital Age***, A/HRC/39/29, Geneva: United Nations Human Rights Council (UNHRC) (accessed 18 September 2021)

UNHRC (2016) ***The Promotion, Protection and Enjoyment of Human Rights on the Internet***, A/HRC/32/L.20, Geneva: United Nations Human Rights Council (UNHRC) (accessed 18 September 2021)

Surveillance Law in Africa: a review of six countries

Egypt country report

Mohamed Farahat

Introduction

Surveillance affects many human rights, including the right to freedom of expression, right to assembly, right to information and communication, and right to privacy. In Egypt, surveillance practices were used before 2011 under the regime of Hosni Mubarak to monitor terrorist activities. Following the key role that social media played during the 2011 revolution and later protests, the regime took specific measures to control access to the internet and target activists with surveillance. Since 2011, different Egyptian regimes have used various technical means to surveil activists and online content. They have used legislation to ban websites, obtain personal data, abuse citizens' right to privacy and criminalise the right to freedom of expression using accusations of fake news.

Although Egypt is party to a number of international conventions protecting citizens' right to privacy, several state agencies are exempt from legislation and there is evidence that the government regularly violates citizens' right to privacy. According to Paradigm Initiative (2019: 15): 'In 2019, a series of sophisticated cyber-attacks targeting the nation's journalists, academics, lawyers, opposition politicians and human rights activists [took place]'. The report added that since that time 'the surveillance activity of government has only deepened and not ceased. A number of the targets of surveillance were then arrested by Egyptian authorities' *(ibid.)*. These surveillance practices and newly adopted legislation led to the closing of civic space in Egypt and abuse of the right to privacy and digital rights (Farahat 2020a).

This report reviews the Egyptian legal framework regulating surveillance practices and examines its conformity with international standards, particularly the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2014). It makes this assessment by answering a series of questions that reflect on surveillance practices in the Egyptian context. The report will first outline the content of existing national legislation and then measure it against relevant international comparators. The report pays particular attention to the parameters within which surveillance is permitted in law and to the legal safeguards detailed in the legislation, before concluding with a number of recommendations.

Communications surveillance has been defined in various ways. In the International Principles, the term refers to 'the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past,

present, or future'. According to article 2(1) of the United Nations (UN) Draft Legal Instrument on Government-led Surveillance and Privacy (2018):[1]

> surveillance is any monitoring, collecting, observing or listening by a state or on its behalf or on its orders of persons, their movements, their conversations or their other activities or communications including metadata and/or the recording of the monitoring, observation and listening activities.

Both definitions refer to the broad definition of surveillance, which includes all practices that constitute surveillance whether directly or indirectly. Therefore, this section of the report will address all related legislation that enables or limits surveillance practices, whether directly or indirectly.

The remainder of this report takes the form of answers to 12 questions.

1 This draft text for a Legal Instrument on Government-led Surveillance and Privacy is the result of meetings and exchanges between the MAPPING project and several categories of stakeholders shaping the development and use of digital technologies. These include leading global technology companies, experts with experience of working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping the Internet and the transition to the digital age.

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

According to principle 1 of the International Principles (legality):

> Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.
> (EFF 2014)

Citizens' right to privacy is protected in Egyptian law. However, state agencies have been given permission to violate this right in specific circumstances. Reasons the government argues justify breaching privacy and carrying out surveillance include national security, states of emergency, terrorism and cybercrime. These are referred to as 'legitimate aims' in the language of the International Principles.

2. Which international conventions protecting privacy has Egypt adopted?

The 2014 Constitution of Egypt (art. 151) states that, 'Egypt is obliged by all international human rights conventions that it has ratified, and they have the same power as the law once published' [author's translation].

International human rights conventions

In the context of privacy, Egypt is party to several international human rights instruments that provide the right to privacy, such as the Universal Declaration of Human Rights (UDHR) 1948 and International Covenant on Civil and Political Rights (ICCPR) 1966. Egypt is also a party to the African (Banjul) Charter on Human and Peoples' Rights 1980 and Arab Convention of Anti-information Technology Crimes (Cybercrimes) 2010.

Table 1.1 Egypt's ratification status

Instruments of the International Labour Organization	Date of signature	Date of ratification
Universal Declaration of Human Rights	1948	
International Covenant on Civil and Political Rights	04 August 1967 (optional protocol not signed)	14 January 1982
International Covenant on Economic, Social and Cultural Rights	04 August 1967 (optional protocol not signed)	14 January 1982
Convention on the Elimination of All Forms of Discrimination against Women	16 July 1980	18 September 1981
UN Convention on the Rights of the Child	05 February 1990	06 July 1990
African (Banjul) Charter on Human and Peoples' Rights	16 November 1981	20 March 1984
Arab Charter on Human Rights		2018
Arab Convention of Anti-information Technology Crimes (Cybercrimes) 2010		8 October 2014
Cairo Declaration on Human Rights in Islam	05 August 1990	

Source: Adapted from University of Minnesota, Human Rights Library[2]

2 http://hrlibrary.umn.edu/research/ratification-egypt.html

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

It is not only the legality principle that the state should adhere to; surveillance should also have a legitimate aim. According to principle 2 of the International Principles:

> Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
> (EFF 2014)

Not only do the key international conventions to which Egypt is party prohibit surveillance and protect the right to privacy, but the Egyptian constitution also emphasises the same rights and obligations. However, domestic laws do not align with these international and constitutional obligations, as is discussed later in this report.

a) 2014 Constitution of Egypt

Privacy of communication is constitutionally guaranteed for all Egyptian citizens. Article 57 of the constitution stipulates that:

> Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed, and they may only be confiscated, examined or monitored by causal judicial order, for a limited period, and in cases specified by the law; the state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law.
> (Arab Republic of Egypt 2014 [author's translation])

According to article 71 of the constitution: 'it is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers and media in any way. In exceptional circumstances, they may be subject to limited censorship in times of war or general mobilization' *(ibid.)*. Despite these constitutional

guarantees some Egyptian laws provide a legal basis for surveillance in certain circumstances.

Egypt has domestic legislation that provides the legal basis for surveillance such as Emergency Law no. 162 (1958), Telecommunications Regulation Law no. 10 (2003), Anti-Terrorism Law no. 94 (2015), Anti-Cyber and Information Technology Crimes (Cybercrime Law) no. 175 (2018) and Personal Data Protection Law no. 151 (2020).

b) Emergency Law no. 162 (1958)

The Emergency Law is one of the legal tools that permits surveillance in the context of a declared emergency. This law is designed to be used only in a state of emergency, which by its nature is temporary, exceptional and for a limited time. However, in Egypt states of emergency have been used on a regular basis and, having been declared, are frequently extended (often multiple times). One is in place at the time of writing this report. Article 3(2) of the Emergency Law stipulates that, 'the President has a right to order surveillance of all messages, whatever their type, and to monitor all means of expression.' Although the constitutionality of article 3 has been challenged before the Constitutional Court (case no. 17/15/2013), the court ruled that searching physical spaces was unconstitutional but made no ruling on digital surveillance.

c) Telecommunications Regulation Law no. 10 (2003)

Article 64(1) of the law prohibits using devices to encrypt communication without permission from security agencies. Article 64(2) stipulates that service providers should collect accurate information and data about service users. Article 67 gives the competent authority power to control all communication services. Prevention of encrypted communication violates citizen's right to privacy and to anonymity.

d) Anti-Terrorism Law no. 94 (2015)

Without clarifying the grounds that justify surveillance, article 46 of the law authorises public prosecutors or 'any other investigating authority' in the case of terrorist crime, upon a justifiable order to surveil, to record conversations and messages; and to record and photograph what happens in private places or via websites for a period of not more than 30 days. The surveillance order is renewable for another period or periods. This means that the surveillance order could be renewed indefinitely, particularly as the law does not identify safeguards for renewing the surveillance order.

e) Cybercrime Law no. 175 (2018)

The law enables state surveillance by requiring all phone and internet service providers to record and store all communications and metadata and to make them available to state agencies. Article 2/first/(1) of the law states that service providers should retain and store information system records for a period of 180 continuous days. The retained information should include: data that can identify service users; and data relating to the contents of the information system used. Article 2(2) adds that service providers should maintain the confidentiality of retained and stored data, including: users' personal data; information relating to the websites and private accounts they navigate and log into; and persons and destinations they communicate with.

Article 6 gives the power to the investigating authority to issue a decision allowing surveillance and access to information. Although individuals have the right to challenge the surveillance order before a court (art. 6(2)), the order can be issued without obtaining prior court authorisation. This means investigating authorities are able to access data possessed by internet service providers relating to all user activities, including phone calls, text messages, websites navigated, and applications used on smartphones and computers.

In a different context, article 25 criminalises breaches of the 'principles and values of Egyptian families', without providing a legal definition of those principles and values. As a result, in July 2020 several Egyptian women were arrested on charges related to this article, now known as the 'TikTok girls' case (Columbia University n.d.).

f) Personal Data Protection Law no. 151 (2020)

The UN Human Rights Committee in its general comment no. 16 on article 17 of the ICCPR states that:

> integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.
> (UNHRC 1988)

Article 3 of the Egyptian Personal Data Protection Law stipulates that 'the law will not apply to the personal data in the possession of national security bodies'. Article 1 identifies the national security bodies as: 'The Presidency of

the Republic, the Ministry of Defence, the Ministry of Interior, the Intelligence Service and the Administrative Oversight Authority'. This means that national security bodies are able to possess all personal data without legal justification.

Although, the legislation's claimed purpose is to protect rights, in practice the Egyptian legal framework has been the strongest tool used to abuse digital rights during the coronavirus (Covid-19) pandemic (Farahat 2020b).

4. How does Egyptian surveillance law compare with that in Africa/US/EU/UK?

The previous sections give an overview of existing national laws regulating surveillance practices, highlighting the key international conventions that Egypt is part of and has used to prohibit communications surveillance. This section uses the Declaration of Principles on Freedom of Expression and Access to Information in Africa as a means to compare Egyptian law against an ideal rights-based approach to surveillance practice.

Principle 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa states that:

> Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information and Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.
> (African Commission on Human and Peoples' Rights 2019)

The Egyptian constitution guarantees the inviolability of private communication and prohibits surveillance (art. 57 and art. 71). However, article 6 of the Cybercrime Law as well as article 3(2) of the Emergency Law authorise the state to breach the right to privacy and enable it to practise surveillance under legal cover.

In addition, principle 4(1) of the African Declaration of Principles on Freedom of Expression and Access to Information in Africa adds that:

> States shall only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards and above-mentioned declaration, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
> (ibid.)

Nevertheless, the Egyptian legal framework does not require any test for reasonable suspicion prior to authorising surveillance targeting communications. Egyptian laws enumerate the circumstances in which

authorities are allowed to target communications. Moreover, article 67 of the Telecommunications Law gives the competent authority the right to control all communications services. According to a report by the **Association for Freedom of Thought and Expression** (2020): '[mobile telecoms operator Orange Egypt] said on its website that it "has the right to disclose all or some of the data and information of its customers if this is in implementation of the law or a decision issued by a competent judicial authority or any of the national security agencies"'.

In the context of principle 42 of the declaration ('Legal framework for the protection of personal information'), Egypt has adopted a legal framework for data protection. Although the law attempts to align with international standards, especially the European Union (EU)'s General Data Protection Regulation (GDPR), the law contains some provisions that contradict the right to privacy, such as article 3, which gives security agencies the right to access personal information without specific restriction. Although Egypt has adopted legislation that is apparently in line with international standards, on closer inspection these pieces of legislation have many legal gaps, as discussed in section 9 of this report.

The International Principles are an additional point of comparison for Egyptian surveillance law. The International Principles were cooperatively drafted by more than 40 international privacy and security experts at a meeting in Brussels in October 2012 and officially launched at the UN Human Rights Council in Geneva in September 2013 (EFF 2014).

When assessing Egyptian laws against the 13 International Principles, it is clear that Egyptian legislation falls short in a number of regards. Gaps exist particularly regarding the principle of legality, which refers to the fact that any surveillance practices should be as prescribed in legislation. Although surveillance takes place according to law, ambiguous provisions and the exemption of some security agencies from the law's applicability make surveillance practices in Egypt illegal. Moreover, Egyptian laws do not align with the principles of necessity and legitimate aim, which refer to the fact that surveillance should have to achieve a legitimate aim (such as preventing terrorist attacks). It is important the legislation defines clearly what are considered to be legitimate aims. The issue of proportionality is also central to the principles. This requires the authorities to weigh the benefit sought from surveillance against the violation of privacy rights. The Emergency Law exempts security agencies from the applicability of the principle of proportionality, and it constitutes the root of all abuses of human rights in Egypt according to Hassanin (2014), who argues that: 'The emergency law seems to be diametrically opposed to the [International Principles]'.

According to the authors of the International Principles (EFF 2014), 'States should enact legislation criminalizing illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties'. In addition: 'States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.'

This principle reflects that:

> the duty of governments to deter unlawful surveillance by way of criminal and civil sanctions reflects the requirements of international human rights law to protect individuals from breaches of their privacy, not only by the state but also by private individuals.
> (ibid.)

According to article 36 of the Personal Data Protection Law:

> the controller and possessor shall be punished with a fine of not less 100,000 Egyptian pounds[3] and not more than 2m Egyptian pounds,[4] [and] anyone who collects, processes, discloses, or circulates any personal data which is electronically processed in non-permissioned cases or without consent of data subject.

According to the same article:

> the punishment will be jail for not less six months and a fine of not less than 200,000 Egyptian pounds[5] and not more than 2m Egyptian pounds or one of these punishments if the purpose was not for material or moral benefit or for the purpose of exposing the data subject to harm and risk.

Article 41 of the same law stipulates that the:

> processor, controller and possessor shall be punished with jail for no less three months and a fine of not less than 500,000 Egyptian pounds[6] and not more than 5m Egyptian pounds[7] or one of these punishments, for collecting, processing, disclosing, circulating, storing and maintaining any sensitive personal data in non-permissioned cases or without consent of the data subject.

3 c.US$6,400.
4 c.US$127,400.
5 c.US$12,800.
6 c.US$31,850.
7 c.US$318,450.

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

As addressed in previous sections, the principles of legality, legitimate aim, proportionality and transparency are key principles that ensure the elimination of unauthorised electronic surveillance. Article 4 of the UN Draft Legal Instrument set out, *inter alia,* principles that ensure that surveillance systems shall be authorised by law prior to use. This law identifies the purposes and situations where surveillance systems are to be used and defines the category of serious crimes and/or threats for which surveillance system are to be used. States should set up and promote procedures to ensure transparency about and accountability for government demands for surveillance data and non-surveillance data for surveillance purposes.

A review of sections 3, 4 and 9 of this report illustrate that Egyptian laws regarding surveillance are not in line with the UN Draft Legal Instrument, specifically in terms of identifying the purposes and situations in which surveillance systems are to be used and defining the category of serious crimes and/or threats for which they are to be used. Moreover, the applicability of the Emergency Law constitutes a permanent legal challenge to the right to privacy and undermines any attempts to combat surveillance practices. Therefore, one of the indispensable recommendations of this report is to amend the Emergency Law to bring it in line with international standards.

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

According to principle 2 of the International Principles (legitimate aim):

> Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. (EFF 2014)

According to principle 3 (necessity):

> Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. (ibid.)

The review of the national laws in section 3 of this report reveals that they do not include an adequate definition of key legal terms or use vague terms. For example, article 1 of the Cybercrimes Law defines national security as: 'everything related to the independence, stability, and security of the homeland and anything related to the affairs of the Presidency, the Ministry of Defence and General Intelligence, and the Administrative Oversight Authority'. The same article and article 1 of the Personal Data Protection Law identifies the national security bodies as: 'The Presidency of the Republic, the Ministry of Defence, the Ministry of Interior, the Intelligence Service and the Administrative Oversight Authority'. Other than these definitions, no existing laws address or explain the definitions of key legal terms such as reasonable grounds, legitimate purpose, etc.

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

Although the existence of the laws ensures the right to privacy and restricts surveillance practices, constituting a legal guarantee, it does not at all demonstrate the efficiency of the laws, particularly if these legal safeguards are not clear or if they are restricted by exceptional laws, namely emergency laws. Article 3 of the Personal Data Protection Law specifies the pre-conditions for collecting data. These include: collecting data for a specific purpose; declaring to the data subject that their collected data will be processed legitimately and explaining the relevance and purpose of collecting their data; and not retaining data for longer than the period necessary to fulfil the purpose of collecting it.

However, article 2/first/(1) of the Cybercrime Law states that service providers should retain and store records of information systems for a period of 180 continuous days. The retained information should include: data that can identify service users; and data relating to the contents of the information system used. Item 2 of the same article adds that service providers should maintain the confidentiality of retained and stored data, including: users' personal data; information relating to the websites and private accounts they navigate and log into; and persons and destinations they communicate with it.

This reflects that legal guarantees in the Personal Data Protection Law directly conflict with the Cybercrime Law.

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

Principle 5 of International Principles (proportionality) states that:

> Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interest.
> (EFF 2014)

As mentioned in the previous section, existing laws are not sufficient to ensure respect for privacy or to eliminate surveillance and they do not consider the sensitivity of information and data. Although Egypt is party to the ICCPR and other human rights conventions that protect the right to privacy guaranteed in the constitution, there is no specific guarantee of privacy written into domestic Egyptian law. Additionally, new legislation about data protection only applies to electronic data and does not address physical data, which means that privacy is still at risk of abuse.

On the other hand, the exception which excludes information in the possession of security agencies from application of the Personal Data Protection Law reflects that the existing laws are not efficient at protecting privacy or limiting surveillance. On the contrary, they allow the expansion of surveillance. For example, existing laws have been used to enable surveillance of social media platforms and to track information posted about Covid-19, which has led to the arrests of many people who have been interrogated for circulating 'fake news' (Farahat 2021b). In addition, the Emergency Law is the main factor in the breakdown of legal guarantees, in contravention of the International Principles (Hassanin 2014).

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

All surveillance is a violation of the right to privacy. However, some surveillance is legal. Legislation can define legitimate aims of surveillance, such as the prevention of serious crimes. These legal boundaries refer to the legality of practices that constitute a restriction on human rights. They aim to protect human rights against arbitrary state practices (EFF 2014).

Article 2/first/(1) of the Cybercrime Law allows personal information to be retained for 180 days, as discussed in sections 3 and 7 of this report. The article does not mention what constitutes a legal and proportionate purpose behind obliging service providers to retain this information for six months.

In conclusion, although being legal, necessary and proportionate are mentioned in some provisions, without clear definition in law it is not possible to apply these tests prior to authorisation. Without transparency in the decision-making process, and publication of statistics on requests and authorisation, it is not possible to verify whether practices are aligned with the intent of legislators or fulfil the International Principles. Moreover, the investigating authority and national security bodies are the only bodies that have the absolute discretionary power to define, determine and assess the legality, necessity and proportionality of surveillance, which creates a state of legal uncertainty. Without independent oversight, the state is judge, jury and regulator.

10. How has surveillance law played out in court in Egypt?

Laws do not operate and are not implemented in a vacuum. How courts apply and interpret the law and identify judicial trends needs to be explored, and this would help evaluate to what extent using litigation in surveillance cases could help to change and improve – in strategic ways – existing laws, practices and surveillance-related policies. Despite the absence of surveillance test cases brought before the courts, it is important to point out two court cases. According to a report by Amnesty International (2014):

> the Interior Ministry calls for tenders for a more sophisticated mass monitoring system which will scan social media networks for 26 topics including defamation of religion, calling for illegal demonstrations, strikes and sit-ins as well as terrorism and inciting violence. However, the full list of topics to be monitored has not been made public, leaving individuals unsure of whether and when their communications will be targeted.

In case no. 63055 (28 February 2017), the plaintiff, Egyptian citizen Mustfa Hussien Hassan, brought a case against the Minister of Interior, asking the court to suspend and cancel the decision of the Minister of Interior to conduct a tender for a social media security risk monitoring software system, known as the public opinion measurement system. Although the administrative judiciary court dismissed the case for procedural errors, the court clearly stated that the contract process for this project had already been completed and had entered into force. What is remarkable about this court decision is that the Ministry of Interior did not deny using a surveillance system and surveillance techniques.

In Constitutional Court case no. 17/2013 the court ruled that article 3(1) of the Emergency Law, which allowed authorities to search and arrest persons without the restriction of the criminal procedure code, to be unconstitutional. This is evidence that the courts could play a potentially significant role in challenging surveillance practices. These two cases highlight the great potential of using strategic litigation as a mechanism to test surveillance practices, which in the long term could assist in amending the laws that enable surveillance.

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

Although personal data protection refers to 'law designed to protect your personal data' (Privacy International 2018: 9), the first article of the Personal Data Protection Law stipulates that data protection law only applies to data that is processed electronically, which means that adoption of the law does not really aim to protect personal data and the right to privacy (Technology & Law Community 'Masaar' 2021: 1). Publishing the executive regulation of law would reveal the exact aim behind adopting the new Personal Data Protection Law. It is doubtful this would change the perception of the law.

Although the Egyptian Personal Data Protection Law resembles international standards on privacy and data protection, the law does not align with these international standards where it exempts security agencies from data protection law. Egyptian law gives security agencies the power to process personal data without the prior consent of the data subject. Collecting, accessing, and processing data do not constitute a breach of the right to privacy if they occur in a legitimate manner, for a legitimate purpose and in a lawful way. However, the existence of the national security exemption significantly weakens data protection and privacy (SMEX 2021).

In the context of principle 42 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa ('Legal framework for the protection of personal information'), Egypt adopted the required legal framework on data protection in July 2020. Although the law attempts to align with international standards, especially GDPR, it contains provisions that contradict the right to privacy; for example, the third article, which gives security agencies the right to access personal information without specific restriction. This supports the conclusion that: 'Numerous Egyptian security agencies are permitted to conduct electronic surveillance, frequently with limited court oversight' (Marczak *et al.* 2015:18).

The Telecommunications Regulation Law constitutes an additional legal challenge, motivating and protecting illegal surveillance practices. Article 64(1) of the law prohibits using devices to encrypt communication services without permission from security agencies. Moreover, article 64(2) of the same law states that the 'services provider should collect accurate information and data about service users' [author's translation]. As a result, some reports

state that: 'Telecommunications surveillance is facilitated under the 2003 Telecommunications Regulation Law' (Marczak *et al.* 2018: 26).

The same report states that:

> This law compels telecommunications operators to provide technical capacity for the military and national security entities to 'exercise their powers within the law' as well as prohibiting the use of 'telecommunication services encryption equipment' without written authorization from entities including the armed forces.
> (ibid.)

In terms of privacy and communication surveillance, article 6 of the Cybercrime Law authorises the investigation authority to issue a decision that allows surveillance and access to personal information. Although the article reveals that it is in line with international standards and principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, in practice there have been many breaches of this provision, with people subjected to searches of their mobile phones without advance permission from the investigation authority; for example, 'police stopping young persons in public places and searching their telephones for evidence of involvement in political activities deemed antigovernment in nature' (US Embassy in Egypt 2021).

There is a clear conflict between article 3 of the Personal Data Protection Law and article 2/first/(1) of the Cybercrime Law, which obliges service providers to retain personal data and data related to online activities, messages and communication. As a result, activists have been interrogated over circulating fake news (Farahat 2021a) about Covid-19; for example, as detailed in State Security cases no. 535 and no. 558 of 2020, involving doctors, journalists, activists, citizens and researchers, which indicate that there was government surveillance of social media targeting users who circulated information about Covid-19 or criticised the performance of government in dealing with the crisis.

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

In conclusion, the existing legal framework in Egypt is not effective at protecting citizens' right to privacy. Existing legislation does not sufficiently define what constitutes a legitimate aim or reasonable grounds for surveillance. It does not provide sufficient clarity about the assessment of whether proposed surveillance is legal, necessary or proportionate. Although the constitution makes citizens' privacy inviolable, and parliament has adopted international conventions expanding and extending these rights, existing laws falls short of the International Principles and the Declaration of Principles on Freedom of Expression and Access to Information in Africa. Therefore, the following actions are strongly recommended.

General

- Surveillance practice should be within very narrow limits. Legality, necessity and proportionality of surveillance decisions and orders should be subjected to prior judicial review. Any exceptional authority for any agency should be suspended immediately. As long as surveillance practices affect human rights, there should be oversight by a competent judicial body.

For the Egyptian parliament

- Parliament should amend or cancel article 2/first/(1) of the Cybercrime Law regarding retaining data for 180 days in a manner that prevents abuse of users' privacy.
- Parliament should amend the Telecommunications Regulation Law and ensure the legitimacy of surveillance practices. It should require that surveillance has an explicit legitimate aim. Courts should be responsible for assessing the existence of a legitimate aim for surveillance and issuing the surveillance order based on their own assessment, giving a person who will be under surveillance the right to challenge the first instance court decision before higher or appeal court.
- Parliament should activate its parliamentary oversight tools to monitor abuses of the right to privacy and illegitimate surveillance practices.
- Parliament should establish a fact-finding committee responsible for investigating surveillance practices and its root causes, which would

report its findings and make recommendations before the whole parliament.

For academia and researchers

- Court cases and decisions related to surveillance practices should be analysed and studied, and judicial trends in this respect should be identified at regional and national levels.
- The impact and potentiality of using judicial bodies to change existing laws, practices and policies should be assessed.

For NGOs

- Capacity-building is required for lawyers and NGOs on using strategic litigation mechanisms nationally, regionally and internationally in surveillance and digital rights cases.
- Public awareness on privacy rights and surveillance practices needs to be increased.
- Concerns should be raised about surveillance practices during universal periodic reviews and via shadow reports.

References

African Commission on Human and Peoples' Rights (2019) ***Declaration of Principles on Freedom of Expression and Access to Information in Africa***, Banjul (accessed 18th September 2021)

Amnesty International (2014) ***Egypt's plan for mass surveillance of social media an attack on internet privacy and freedom of expression*** (accessed 4 August 2021)

Arab Republic of Egypt (2014) Egyptian Constitution, *Official Gazette* issue 3 (bis)A, 18 January

Association for Freedom of Thought and Expression (2021) ***The Internet and the Law in Egypt Series*** (accessed 4 August 2021)

Columbia University (n.d.) ***The Case of the Egyptian TikTok Influencers*** (accessed 4 August 2021)

Electronic Frontier Foundation (EFF) (2014) ***Necessary & Proportionate: The International Principles on the Application of Human Rights to Communications Surveillance*** (accessed 18th September 2021)

Farahat, M. (2021a) ***Coronavirus Trials in Egypt: Blurring the Lines Between Fake News and Freedom of Expression***, SMEX (accessed 4 August 2021)

Farahat, M. (2021b) Egypt Digital Rights Landscape Report, in T. Roberts (ed.), ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries,*** Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.014**

Hassanin, L. (2014) *Global Information Society Watch 2014*, APC and Hivos

Marczak, B; Dalek, J.; McKune, S.; Senft, A.; Scott-Railton, J. and Deibert, R. (2018) ***Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?***, Citizen Lab Research Report No. 107, University of Toronto (accessed 18th September 2021)

Marczak, B.; Scott-Railton, J.; Senft, A.; Poetranto, I. and McKune, S. (2015) ***Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation***, Citizen Lab Research Report No. 64, University of Toronto (accessed 18th September 2021)

Organisation of African Unity OAU) (1981) *African (Banjul) Charter on Human and People's Rights*, OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), Banjul

Paradigm Initiative (2019) *Digital Rights in Africa Report 2019,* Lagos: Paradigm Initiative

Privacy international (2018) ***A Guide for Policy Engagement on Data Protection – Part 1: Data Protection, Explained*** (accessed 4 August 2021)

SMEX (2021) ***Data Protection and Privacy Laws in MENA: A Case Study of Covid-19 Contact Tracing Apps***, Social Media Exchange Association (accessed 4 August 2021)

Technology & Law Community 'Masaar' (2021) ***Personal Data Protection Law: Does it Really Aim at Bolstering the Right to Privacy? Or is it an Attempt to Give the Illusion of an Improvement in the Legislative Environment?*** (accessed 4 August 2021)

United Nations Human Rights Committee (UNHRC) (1988) CCPR General Comment No. 16: Article 17 (Right to Privacy), ***The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation***, 8 April (accessed 2 July 2021)

US Embassy in Egypt (2021) ***2020 Country Reports on Human Rights Practices: Egypt, Bureau of Democracy, Human Rights, and Labor*** (accessed 4 August 2021)

Surveillance Law in Africa: a review of six countries

Kenya country report

Grace Mutung'u

Introduction

This report provides an overview of the legal basis for government surveillance and protections of citizen privacy in Kenyan law. The report summarises the most relevant pieces of legislation and compares them to existing law in other countries and draft legislation and principles provided by human rights actors. The report focuses particular attention on circumstances in which surveillance is legally permitted, as well as checks and balances detailed in legislation. The final section makes a series of recommendations arising from this analysis for future legislation, legal practice and further research.

Kenya has had a long history of surveillance practices, inspired by the need for social control during the colonial and post-colonial periods, motivated in recent years partly by anti-terrorism, anti-money laundering and public health initiatives. During the colonial period, the government appropriated intelligence systems from various Kenyan communities as part of its colonial conquest. For example, elders would send people pretending to be mad, herders or lost strangers to check out the military strength of other communities or fertility of lands they were interested in (Boinett 2009: 18). Thereafter, the colonial government developed surveillance practices to monitor and counteract dissent. These included fingerprinting of Africans and requirements for movement passes (Breckenridge 2019).

Apart from fingerprinting of the indigenous population, surveillance of persons of interest also dates back to the colonial period. The colonial government in Kenya had an elaborate administrative structure whose duties included gathering intelligence. The police force, established in 1906, also carried out surveillance. Following increased unrest and resistance in the 1920s, a criminal investigations department was established in 1926. One of its duties was to collate data on 'criminals, undesirable and suspicious persons'. It was later mandated to carry out intelligence, and passport and immigration control, as well as fingerprinting. Eventually, a unit known as the 'special branch' was carved out within the department for covert operations and intelligence gathering (Boinett 2009).

At independence, Kenya inherited these surveillance practices. Constitutional changes resulted in a centralised government that maintained colonial administrative structures. The special branch acquired immense power as the intelligence outfit of the central government. It is most infamously remembered for monitoring dissenters in all sectors of society, extrajudicial killings and a disregard for human rights (*ibid.*: 26). The special branch was dismantled and a national intelligence service established under a 1998 law. These experiences informed provisions in the new Constitution of Kenya.

During the constitution-making process at the beginning of the twenty-first century, several constitutional provisions spelling out the powers and limits of national security organs were included. Article 239 of the Constitution defines national security organs as the Kenya Defence Forces (KDF), National Intelligence Service (NIS) and National Police Service (NPS). The organs are supervised by the National Security Council (NCS). A provision on how fundamental rights and freedoms could be limited was also made (Constitution of Kenya 2010, article 24).

Since 2013, Kenya has suffered several terrorist attacks by militant Islamist group Al-Shabaab. The attacks revived the agenda to strengthen the national security apparatus (Lind, Mutahi and Oosterom 2015). In 2014, following several terrorist attacks in northeastern Kenya, the executive sponsored a bill amending various security laws to give national security organs a legal basis for communications surveillance. The surveillance extends to the financial system, where financial institutions closely monitor and report cash flows; and security operations, where law enforcement bodies have wide latitude to investigate suspected crimes and undertake covert operations. Surveillance extends to anti-corruption initiatives; and there are also regulations for mandatory mobile phone SIM card registration and proposals to whitelist all mobile devices, including phones (Republic of Kenya 2015; Communications Authority 2018).

Kenya also has massive data sets that can be used for surveillance purposes. For example, under the Registration of Persons Act, every person is required to register for an identity card on reaching the age of 18. In 2019, the government transformed the register under the Act to a digital identity system known as the National Integrated Identity Management System (NIIMS). Popularly known as *huduma namba*,[1] the system collates and centralises all identity profiles and identity processes issued and carried out by government agencies. Subsidiary laws under NIIMS mandate issuing a unique personal identifier to each person – citizens, residents and even children. The number – together with biometrics such as fingerprints and iris, earlobe and facial photographs – is required for identification and authentication, prior to accessing government and private services. This could arguably become the most comprehensive surveillance system in Kenya, if the government integrates data sets from government identity systems under *huduma namba* with private data such as mobile phone numbers and social media. It was noted in a judgement following a case contesting *huduma namba* that the government needed to enact an appropriate comprehensive regulatory framework to ensure legal protections (eKLR, 2020b: para. 1047(III)).

1 Swahili for 'service number'.

However, civil society organisations have criticised the Kenyan government for conducting extra-legal surveillance and intercepting communications (Privacy International 2017). They have also raised concern about surveillance of groups such as people with HIV or AIDS, human rights defenders and children (UPR Info 2020; eKLR 2020b: para. 791). In addition, private companies such as mobile network operators have been reluctant to install systems that would give government actors access to subscriber information on their networks. These include the 2012 International Telecommunication Union-supported Network Early Warning System (NEWS), which operators argued would disproportionately affect subscriber privacy, as well as the 2018 Device Management System (DMS), which the communications regulator wanted installed to weed out counterfeit devices. In the case of the DMS, mobile network operator Safaricom was among the parties that went to court to oppose the system, arguing that anti-counterfeiting goals could be achieved using less invasive measures (eKLR 2020a).

This report reviews the legal basis for legitimate surveillance in Kenya and protections provided in law for citizens' right to privacy. It does so by answering a series of 12 questions about surveillance law in Kenya.

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

Motivations for surveillance include prevention of terrorism and serious crimes, national security, anti-corruption, health emergencies and control of hate speech, particularly during election periods. All these are provided for in various laws and practices, which have been developed with local and external influences. For example, following a United Nations (UN) Security Council resolution on suppression of terrorism, Kenya introduced mechanisms for the surveillance of terrorism financing (Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations 2013). Further anti-terrorism-inspired laws were made in December 2014 under the Security Laws Amendment Act. The statute amended several security-related laws to provide for surveillance of persons suspected of serious crimes, as well as terrorism. Finance laws were also amended to strengthen know-your-customer measures, as well as reporting requirements for financial institutions, payment service providers and foreign exchange bureaus.

Under the National Intelligence Service (NIS) Act 2012, protection of national security is among the main reasons for intelligence surveillance. Other rationales for surveillance include prevention of crime and keeping of law and order (National Police Service (NPS) Act 2011, section 51(g)). Anti-corruption and prevention of economic crimes is also cited as a basis for surveillance, although this is not specifically provided for in the anti-corruption law.

Another motivation for surveillance is to protect intellectual property. Private actors such as content owners have attempted to have internet service providers and mobile network operators monitor their networks for content that infringes on their intellectual property rights (Article 19 Eastern Africa 2020). The Communications Authority in 2017 attempted to install a DMS that would connect to mobile network operators' systems to filter out counterfeit devices in the country. The High Court in 2018 declared DMS unconstitutional, but later in 2020 the Court of Appeal allowed the DMS project to recommence and ordered the Communications Authority to subject the proposed DMS guidelines to public participation (eKLR 2020a).

Health surveillance is carried out under the Public Health Act 1986, which was enacted during a time when digital surveillance had not been anticipated. Since the emergence of Covid-19 in Kenya in 2020, the Ministry of Health,

with the aid of the NIS, has been undertaking health surveillance, reportedly through a system that helps with contact tracing (Odhiambo 2020). The Public Health Act does not specifically provide for contact tracing. Initially, the state tracked Covid-19 patients as well as people under quarantine, to ensure that they did not flout movement restriction rules (Olewe 2020). Along the way, a digital tracing app that used geolocation data to track people passing through the country's airports and ports was deployed. Currently, Kenya is collaborating with African health authorities in sharing information about Covid-19 testing and vaccination certification for travellers (Amoth 2021). The Ministry of Health also has a vaccine management system linked to the national identity (ID) card system. This system is among use cases for the national ID, which is increasingly becoming digitalised.

2. Which international conventions protecting privacy has Kenya adopted?

Article 2 of the Constitution of Kenya incorporates international law and obligations as part of domestic law. Kenya has signed the Universal Declaration of Human Rights (UDHR) and ratified the International Covenant on Civil and Political Rights (ICCPR), both of which confer on all citizens the right to privacy and to private correspondence and communication. Regionally, Kenya is also a signatory to the African Charter on Human and Peoples' Rights (ACHPR). Although the ACHPR does not specifically provide for the right to privacy, it provides for dignity of individuals and groups to pursue their development (African Union 1981: articles 5 and 24). Along with other members of the East African Community (EAC), Kenya adopted the EAC Framework for Cyberlaws Phases I and II in 2008 and 2011 respectively (EAC 2008). These frameworks envisage a harmonised cyber environment, with each country expected to adopt laws on data protection as well as cybersecurity.

Kenya has also signed and domesticated UN conventions aimed at addressing terrorism and terrorism financing; and established a financial reporting centre, as well as the Counter Financing of Terrorism Inter-Ministerial Committee under the Prevention of Terrorism Regulations. These regulations create a basis for financial surveillance and reporting.

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

Kenya does not have a specific law regulating surveillance, but several laws either prohibit or regulate surveillance. At the highest level, the Constitution protects privacy, including informational privacy. Article 31 frames the right to privacy as including protection from: search and seizure of property; information about family or private affairs being unnecessarily required; and infringement of communications. In addition, article 35 guarantees citizens' right to access to information. This includes information held by the state and others that is necessary for the enjoyment of rights or freedoms.

Both the right to privacy and access to information are among the fundamental rights that can be limited through legislation. Article 24 of the Constitution lists the factors to be taken into account when limiting a right. These include the: nature of the right; purpose of the limitation; nature and extent of the limitation; and a balance between individual enjoyment of rights and the rights and fundamental freedoms of others, whether less restrictive measures to limit the right exist or not. In addition, the Constitution allows for limitation of the right to privacy, among other rights, for members of the Kenya Defence Forces and the NPS (Constitution of Kenya 2010, article 24). For example, police officers' right of access to information is limited, under several justifications, such as protection of classified information, national security, security and integrity of the police service as well as protection of the fundamental rights of others (NPS Act 2011, section 47(2)).

For access to information related to surveillance, the Access to Information Act sets out reasonable grounds under which an access to information request may be denied. These range from national security interests to due process, protection of the privacy of others, protection of commercial interests, including intellectual property, and professional confidentiality (Access to Information Act 2016, section 6). The law further outlines what 'national security' consists of, which includes covert operations, intelligence activities and lawful investigations. However, the law includes a public interest test, where a court may order disclosure of information if the public interest outweighs the harm to protected interests. In addition, requests for information relating to environmental tests override protected interests (Access to Information Act 2016, section 6(4)).

Statutes on surveillance can be broadly classified into laws that prohibit surveillance and those that allow it.

a) Laws prohibiting surveillance

The Kenya Information and Communication Act (KICA) is the primary law on telecommunications and broadcasting. Section 31 penalises unlawful interception of communication by service providers. Section 83 also creates the offence of accessing computer systems for purposes of interception of communication. Consumer protection regulations under KICA also prohibit licensees from monitoring communications.

Unauthorised interception is prohibited under the Computer Misuse and Cybercrimes Act (CMCA) 2018, with stiff penalties of up to 20 million Kenyan shillings (about US$200,000) (section 17). There is also a new crime of interception of mobile money messages in section 31 of the CMCA.

Kenya in 2019 enacted the Data Protection Act, which regulates lawful processing of personal data. The Act generally prohibits processing of personal data without data subjects' consent (section 30).

b) Laws allowing surveillance

The laws allowing surveillance are varied, ranging from communications regulation to anti-money laundering, security and content regulation statutes. More recently, e-government services such as a national system for schoolchildren and a digital ID programme have created databases for easy surveillance.

KICA has provisions for court-mandated search and seizure where a person is suspected to have committed an offence (section 89). Law enforcement officers often rely on this provision to access information from mobile network operators, which are licensed under this Act (Safaricom 2019).

The main law regulating financial surveillance is the Proceeds of Crime and Anti-Money Laundering Act 2009. Financial institutions are required to monitor patterns of cash flowing into financial reporting centres. They must also verify customer identities, keep records of customers, and establish and maintain internal reporting procedures. This has created the basis for electronic surveillance of financial transactions. It has also led to a push for digital ID, which financial institutions can use to validate their customers' ID documents (Breckenridge 2019).

The NIS Act limits the right to privacy by allowing for court-warranted investigations into suspected crimes. Warrants may be issued for monitoring of communications (section 36A). Although the provision does not specify the offences for which surveillance may be undertaken, provisions for court

warrants under the Act are linked to covert intelligence operations. The NIS Act broadly defines offences that may attract covert operations as any 'threats against national security' (section 42). In terms of proportionality, the provision gives broad powers to monitor communication for purposes of preserving national security. Political leaders, as well as Parliament, have severally proposed or directed NIS to carry out intelligence operations on issues such as impropriety in public service, cheap imports in the agricultural sector and public fundraising (Ombati 2020; Otieno and Obala 2020; Ng'ang'a 2021). The provision on covert operations, however, requires a court to issue a warrant before monitoring of communications can begin. A court can only issue an order for surveillance for 180 days, but this can be extended.

Security laws that allow surveillance include the Prevention of Terrorism Act (PTA) 2012, NPS Act, NPS Commission Act, CMCA and Mutual Legal Assistance Act. The PTA permits the investigation and interception of and interference with a person's communications in the course of investigating, detecting or preventing a terrorist act (sections 35, 36 and 36A). Such interception can be carried out by various bodies, with varying levels of adherence to the principle of proportionality. When carried out by the police, there is a pre-authorisation procedure, involving approval by the inspector general of police or director of public prosecutions, as well as a court warrant.

The law also directs the court to analyse the necessity of the application for a warrant, especially since the application for a warrant may be carried out by the police without involving the subject of surveillance. The law also criminalises unauthorised interception by a police officer. However, in a separate provision, the same law authorises interception of communications by national security organs[2] to intercept communications in 'detecting, deterring and disrupting terrorism' (section 36A). This provision does not further delineate how necessity and proportionality are to be achieved, although it empowers the cabinet secretary to make regulations to give effect to the provision.

Under the NPS Act 2011 and NPS Commission Act 2011, the police can collect and provide intelligence on crimes and undertake investigations on serious crimes including cybercrime. The Act further makes provisions for the classification of information (NPS Act 2011, sections 24, 27, 35 and 51).

The CMCA envisages court-warranted interception of 'content data', defined as the substance of a communication, by law enforcement officers in the course of investigating crimes. Under section 53, officers are expected to procure court orders that can also extend to service providers, which

2 Article 239 of the Constitution defines national security organs as the KDF, NIS and NPS.

may be compelled to help with investigations. Section 52 envisages real-time collection of electronic traffic data, where service providers can be compelled to permit law enforcement officers to collect data. Requests for real-time traffic data, as well as content data, can also be made under mutual legal assistance arrangements;[3] these are not locally authorised by courts (sections 63 and 64).

However, the Mutual Legal Assistance Act contains some necessity and proportionality requirements. For interception requests, the Act requires that the requesting state give information on: the criminal conduct under investigation; identification of the subject, with details for the electronic or telecommunication address to be monitored; desired duration of the interception; and the authority requesting the interception. A confirmation of a warrant or lawful interception order from the requesting country is also required. The Act does not provide any other oversight for mutual legal assistance requests; yet once a request is accepted, Kenya may immediately require immediate transmission of interceptions or recording and subsequent transmission of communications to the requesting state (Mutual Legal Assistance Act 2011, section 27).

Content regulation statutes such as the CMCA and the National Cohesion and Integration Act (NCIA) 2008 establish offences that law enforcement bodies use as a basis for surveillance. The CMCA has established offences such as publication of fake news and spreading of false information, while the NCIA prohibits content that may incite ethnic hatred. The NCIA was passed following post-election violence in 2007–08 that led to the deaths of more than 1,200 people and displaced over 500,000. The National Cohesion and Integration Commission (NCIC), which is charged with implementing the NCIA, has invested in surveillance software to monitor election campaign content online (The Nation 2011). During election periods, monitoring of online spaces occurs to identify content that could lead to violence. In 2017, the Communications Authority, in collaboration with the NCIC, issued guidelines on election campaign content disseminated through electronic networks (Communications Authority and NCIC 2017). This was the basis for monitoring SMS text messaging services and social media for what they termed undesirable content. However, there is no specific law mandating digital surveillance for hate speech.

3 Mutual legal assistance is a framework under which a state may request for assistance from another state during criminal investigations. In Kenya, such arrangements are governed under the Mutual Legal Assistance Act 2011, where legal assistance is available to states and international organisations that Kenya has signed agreements with and, in some cases, requesting states, even when there is no prior mutual legal assistance agreement (section 3).

During the Covid-19 pandemic, surveillance has been carried out under the Public Health Act 1986 (section 67). Examples of digital health surveillance include a contact tracing app that integrated public service vehicles (PSV). PSV operators were required to enrol their vehicles on the app using registration numbers and to collect identification card numbers and contact details from every passenger (Oketch 2021; Phillips 2021). The system was later dropped, but other systems (e.g. a testing and vaccine certification system) have been adopted. Civil society organisations have raised concerns over the lack of a legal framework to address the privacy of those whose data is collected, as well as oversight of such surveillance (article 19 2020; Article 19 Eastern Africa, the Kenya ICT Action Network and Pollicy 2021). In the Covid-19 pandemic, people found to be spreading information that was contrary to government reports on both open platforms and private messaging apps were charged with spreading false information under the CMCA (Article 19 2020).

Identity data can also enable government surveillance. The Ministry of Education manages the National Education Management Information System (NEMIS), which records information on all learners in Kenya, including their educational activities. The system issues learners with a unique personal identifier, using their birth certificates and parents' national identity card numbers (Ministry of Education 2017). It is not clear if the system is linked to any other system – for example, *huduma namba* – though law enforcement officers have warned students caught breaking the law that their details will be recorded (Muchunguh 2021).

NEMIS was a precursor of NIIMS, a more comprehensive database that is meant to cover all citizens and residents in Kenya. NIIMS was established in 2019 under the Registration of Persons Act. Subsidiary legislation issued in 2020 makes NIIMS the primary source of identification of all Kenyan citizens/residents in Kenya. This means that through NIIMS, the government can track all the services that a person accesses, from birth to death; for example, mobile phone registration, land registration, health insurance, school enrolment, national examinations and driving records. while the Data Protection Act 2019 prohibits processing of data without the data subject's consent, the Act also lists duties carried out by public bodies as among exceptions to processing without consent. Other exceptions include public interest and exercise of official authority.

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

The provisions prohibiting surveillance in Kenya – starting from the constitutional provisions on privacy, access to information and limitation of rights – measure up to international standards such as the UDHR, ICCPR and ACHPR. They guarantee protection of fundamental freedoms including the right to privacy. Under article 24 of the 2010 Constitution, laws limiting fundamental rights are required to pass the three-part test of legality, necessity and proportionality. This test, which is elaborated under the Constitution, has been the subject of many lawsuits, with judges testing the laws against considerations such as the nature of the law, whether less repressive means could have been used to achieve the same ends, and whether the law is appropriate for a democratic society.

There is no single law that comprehensively regulates surveillance as is the case in South Africa, the United States (US) and the United Kingdom (UK). However, from the various security legislations – for example, the NIS Act, NPS Act and PTA – a primary reason for surveillance is national security. This is similar to many African countries where intelligence gathering is carried out for protection of national security. Other reasons for surveillance include prevention and investigation of crimes, as well as preventing and countering terrorism.

Without a comprehensive law, surveillance practices go on without a legitimate basis or any oversight. These include mandatory SIM card registration, hate speech monitoring and content regulation in general. This is similar to many other African countries where governments undertake surveillance without specifying a legitimate basis and without oversight (CIPESA 2019: 6).

Similar to the US, where the USA PATRIOT[4] Act was adopted as an anti-terrorism measure, Kenya has enacted the PTA as well as regulations on financial reporting as part of the war on terror. However, as has been argued in cases such as the Coalition for Reform and Democracy (CORD) case, anti-terrorism efforts can easily give rise to mass surveillance as state agencies can use investigation of terrorism to gain access to mobile, internet and financial records (eKLR 2015). The case challenged a raft of amendments to

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

security laws where the state sought to enhance anti-terrorism investigation by detaining terrorism suspects without charging them, limiting expression and creating a legal basis for covert intelligence operations.

In terms of oversight, Kenyan law has similarities with South African law with regard to seeking administrative and judicial approval of warrants for surveillance. Under the NIS Act, court warrants are required prior to covert operations, similar to the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act *(RICA)* in South Africa. However, the reporting mechanisms differ, in that Kenya has no specific reporting requirements for surveillance activities to parliamentary committees as is the case in South Africa.

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

The UN Draft Legal Instrument on Government-led Surveillance and Privacy recommends that states have a specific statute and oversight on government-led surveillance. The instrument considers surveillance as a limitation to privacy, requiring states to adopt necessity and proportionality in surveillance. Kenya partly aligns with the draft instrument with regard to the intelligence law, but fails in many other respects, including use of digital identity data for surveillance.

Although there is no single statute regulating surveillance, Kenyan laws enacted immediately after the 2010 Constitution – for example, the NIS Act, NPS Act and PTA – acknowledge that surveillance is a limitation to rights such as privacy and access to information. Where a court has authorised surveillance, the laws require an application to the court to list the reasons why law enforcement officers need to infringe on people's privacy.

Use of digital identity data for surveillance has not been well captured in the laws. For example, there are mandatory SIM card registration laws, where the SIM card is linked to the national ID. However, national ID laws do not provide principles or data-sharing codes among civil registries in the country. Civil registries is a term introduced under *huduma namba* regulations. It refers to government agencies that issue identity documents such as birth certificates, passports and education certificates. Since the registries perform duties of a public nature that may be subject to exceptions to the grounds for data processing, it is important that use of their data for surveillance purposes be regulated.

Kenya's surveillance activities often take place under the veil of national security, an area that has traditionally been protected from public scrutiny. The 2010 Constitution defines national security very broadly, encompassing 'internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests' (Constitution of Kenya 2010, article 238(1)). National security is one of the bases for intelligence operations under the NIS Act. National security is also exempted from the Data Protection Act under section 51.

The NIS Act does not provide a specific oversight mechanism for surveillance, but it does provide three mechanisms for oversight of intelligence in general.

The first is a council consisting of three cabinet secretaries, the attorney general, director general of the intelligence service and any other person the president may appoint. The second is parliamentary oversight and the third is a complaints board. The complaints board, which is headed by a person who may serve as a judge, is mandated to receive complaints from any member of the public (NIS Act 2012, pt. VII). The UN Draft Legal Instrument and International Principles on the Application of Human Rights to Communications Surveillance call for an oversight mechanism specific to surveillance that is independent of government and security services; and which has the power to access all surveillance requests and authorisations to verify whether surveillance practice is 'legal, necessary and proportionate' as the Act intended.

While the new laws provide for judicial pre-authorisation, this only occurs in specific cases. The Independent Policing Oversight Authority (IPOA) has a mandate to investigate complaints regarding the police. It is made up of a board of experts from various fields. IPOA annual reports highlight the nature of cases the authority has dealt with since its establishment in 2012. Surveillance is not among the complaints, although complaints such as enforced disappearance can be traced to surveillance (Privacy International 2017). IPOA, along with other human rights institutions, could be strengthened through capacity building on issues of surveillance, to be able to play the role of independent oversight body. Also, laws do not provide for the specifics of surveillance, hence there are no guidelines on any of the surveillance systems in use. There are no recorded human rights impact assessments, even for non-surveillance data such as digital ID.

The right to notification that you have been subject to surveillance – recommended in the UN Draft Legal Instrument and the International Principles on the Application of Human Rights to Communications Surveillance – is not provided for in Kenyan surveillance law. While notification is provided for under data protection laws, surveillance may fall under exceptions to the Act as it is undertaken as a public duty (Data Protection Act 2019, section 51(2)(b)). In addition, the law came into force in 2019 and is in the early stages of implementation. Data subjects have not been provided with mechanisms for asserting their data rights. The right to human assessment in automated decision-making processes is also provided for under the data protection law. However, the public is not aware of decisions which are made by automated means or their right to have such decisions subjected to human assessment. Matters of cross-border data transfer are also provided for under the Data Protection Act.

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

The NIS Act defines national security with reference to the constitutional definition. This definition also applies to all other laws on surveillance. The law specifies privacy rights that are limited and outlines 'purposes for the limitations' in part IV. These include: national security; protection of classified information; discipline and security of intelligence officers; and protection of fundamental freedoms of a person which does not prejudice the rights and freedoms of others (section 32).

Section 48 of the NPS Act provides for limitations of the right to access to information, for similar purposes as described under the NIS Act.

Other key legal terms such as reasonable grounds and legitimate purpose are not defined in law but have been considered by courts. For example, Kenya's experiences with terrorism in the country have created the basis for considering the prevention of terrorism to be a legitimate aim of conducting surveillance. In the wake of terrorist attacks, the 2014 Security Laws Amendment Act was enacted. In a case contesting increased risk to privacy under the NIS Act, the court found anti-terrorism intelligence to be rationally connected to the purpose of 'detection, disruption and prevention of terrorism' (eKLR 2015: para. 308). In this particular case, the High Court found that the provisions for internal pre-authorisation as well as requirements for judicial warrants would provide adequate opportunity for the judicial officer to ensure that there were legitimate aims and reasonable grounds for surveillance.

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

Existing safeguards such as constitutional and legal provisions have been removed from public scrutiny since there is no mechanism for independent oversight and public reports. This lack of transparency prevents the public from understanding the full extent of surveillance in the country. Reports indicate that Kenya undertakes surveillance, although it is not possible to know the extent to which the law, or international standards such as the UN Draft Legal Instrument, or necessary and proportionate principles are adhered to. Since 2012, the Communications Authority has attempted to install two systems, NEWS and the National Intrusion Detection System (NIDS), on internet service providers' servers. As reported by Privacy International (2017), the surveillance potential of the systems is not proportionate to the stated benefit, which is to monitor cyber threats.

Another example of a system installed without a proper legal framework is the street-level closed-circuit television (CCTV) surveillance system in the capital Nairobi and in Mombasa. The system was installed by mobile network operator Safaricom in collaboration with Chinese telecoms technology manufacturer Huawei. It includes facial recognition technology as well as licence plate readers (Kapiyo and Githaiga 2014; Burt 2018). Despite protests from civil society organisations, there has been no transparency on use of the system and reports indicate that it is running (Mutai 2020). The system was enhanced by integrating all national security communications systems (The Presidency 2020). Regulations on CCTV use were also put out for public consultation but have yet to be gazetted (Ministry of Interior and Coordination of National Government 2019).

Reports on data use for political campaigning during the 2017 elections indicate that political parties obtained data from public and private databases for targeted advertising (Mutung'u 2018). Use of corporate surveillance for political gain undermines democracy, particularly where the incumbent administration also has political control (Nyabola 2020).

National security has often been used as a reason for not openly discussing surveillance practices. For example, in the 2020 statutory annual report on the state of security, the government reported that it had increased surveillance of online spaces to combat threats such as ethnic hatred, student unrest and counterfeit goods. However, further information – such

as on the systems used, action taken against persons of interest, and safeguards – was not provided (Kenyatta 2020: ix, 13, 17).

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

Although Kenya has constitutional provisions on the right to privacy and access to information, as well as laws on surveillance, these frameworks have not been sufficient to protect the public from unwarranted surveillance. According to a report by Privacy International (2017), law enforcement officers gained access to mobile network operators' data to carry out surveillance on persons of interest. The report tied this surveillance to extrajudicial killings, which led to calls for privacy laws.

However, the Data Protection Act 2019 exempts national security functions from its application. This leaves gaps in areas such as public and private CCTV cameras, which law enforcement agencies can gain access to in the course of their duties, without proper oversight.

The Data Protection Commissioner developed guidelines on data-sharing by private and public entities during the Covid-19 pandemic. However, it is not clear if the guidelines are in operation and there are no records on data-sharing agreements during the pandemic period. This points to the need for the kind of annual public transparency reports recommended by the **International Principles on the Application of Human Rights to Communications Surveillance,** so that citizens and parliamentarians can have confidence that surveillance is being applied in accordance with the law.

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

The Constitution defines national security as 'the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests' (Constitution of Kenya 2010, article 238). This provision was included during the making of the 2010 Constitution to safeguard against the practice of government overreach affecting human rights on grounds of national security.

Laws made pursuant to national security interests have been the subject of constitutional interpretation, with courts generally supporting national security-related activities unless they violate citizen's rights. For example, following a spate of terrorist attacks in the country from 2013, the government amended several security laws with the aim of specially investigating and prosecuting terrorism cases. In a case instituted by the Coalition for Reform and Democracy (CORD) political party and others, the petitioners argued that the amendments severely affected fundamental rights and freedoms such as privacy, access to information and the right to a fair trial. The court found the sections related to access to justice – such as issues of bail, the right to remain silent and access to evidence to be used against the accused – to be unconstitutional. However, limitations on privacy were found to be justifiable in the fight against terrorism (eKLR 2015).

Lack of transparency or reporting mechanisms make it difficult to analyse how judges have considered surveillance applications from law enforcement. Data from private internet service providers on government requests for access to personal data would also be useful in analysing whether surveillance requests are based on law and whether they are necessary and proportionate.

10. How has surveillance law played out in court in Kenya?

Besides the CORD case, other landmark cases include one challenging the collection of data on HIV-positive people, the petition against the DMS and the *huduma namba* digital identity (NIIMS) case. In the first two instances, the courts ruled in favour of the petitioners, upholding the right to privacy. These two cases were instituted following plans by public agencies to create systems for surveillance. In the third case, which concerned a digital ID system, the court seemed to resign itself to the fact that the country must digitalise. It allowed the system, but ordered that a sufficient and comprehensive framework on issues such as protection of privacy be enacted first.

In 2016, President Uhuru Kenyatta directed national government administrators to collect data on HIV-positive people in their jurisdictions, including children attending school, to streamline the supply of HIV medication. The Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), a non-governmental organisation (NGO), challenged the directive on grounds of its proportionality, among other reasons. The organisation argued that collection of biometric data was a violation of privacy that could consequently lead to criminalisation and stigmatisation of already vulnerable people. The court found that, although the government had a legitimate interest, the means of collecting data infringed on people's privacy. Therefore, the directive was declared unconstitutional and the government was ordered to code data that had already been collected (eKLR 2016).

In the DMS cases, mobile network operators and civil society activists protested against the DMS that would have been installed on mobile network operators' systems, to check the authenticity of mobile devices to rid the country of counterfeit devices (Communications Authority 2016). They argued that the system was disproportionate to the mischief the government wanted to cure. The High Court also found that the measures were not necessary because less invasive measures were available that achieved the same ends without violating mobile subscribers' privacy. This decision was, however, subsequently overturned by the Court of Appeal, which ordered the Communications Authority to engage in consultations and also develop guidelines for the project (eKLR 2020a).

Issues of surveillance were part of the CORD case. Petitioners argued that introducing a new provision allowing the NIS to carry out covert operations and interception of communications by national security organs legitimised mass surveillance (eKLR 2015: para. 282). The court, however, took judicial notice of the terrorist attacks that had taken place in the country and found that there was a genuine national security interest – a 'legitimate aim' in the language of the international principles – in monitoring communications to prevent further attacks. With regard to intelligence, it found that the pre-authorisation by a judge, time-limited warrants and criminalisation of unlawful surveillance were sufficient safeguards to privacy. The court emphasised that, given the nature of terrorism, it was justifiable for the government to carry out surveillance, after obtaining court orders. In addition, the court found that the parties had not demonstrated less restrictive ways of achieving the national security purposes of the surveillance law (*ibid.*: para. 308). Notably, petitioners in the CORD case did not canvass issues of oversight and accountability of surveillance. As was the case in the South African case *AmaBhungane Centre for Investigative Journalism v. Minister of Justice and Minister of Police,* the court decried the opaque nature of surveillance orders (Constitutional Court of South Africa 2021).

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

The right to privacy under Kenya's Constitution is well provided for. It includes privacy of information as well as communications. Further, the Constitution has domesticated the legitimacy, necessity and proportionality principles under international law by providing guidelines on how rights such as privacy may be limited. However, the laws under which surveillance is undertaken do not always provide a legitimate basis for surveillance.

Issues of surveillance have been the subject of litigation and courts have upheld the right to privacy in some cases. However, litigation cannot be a sustainable means of protecting the rights of people, with increasing government-led surveillance. A comprehensive law is therefore needed to narrowly define legitimate grounds for surveillance.

Where the private sector is involved, transparency reports by technology companies such as Google are important in bringing to the fore issues of surveillance. People would otherwise not be aware that law enforcement officers surveil their private communications or have any means of appeal or redress. However, not all companies provide reports and, even in the case of Google, not all requests for information are published (Google 2021).

National human rights institutions such as the Kenya National Commission on Human Rights (KNCHR) have not been pursuing digital rights. For example, annual and general reports of such institutions in the past few years have not highlighted the impact of electronic surveillance on fundamental rights. While a 2021 submission to the UN Human Rights Committee raised concerns about the implementation of the PTA being used to shrink civic space, it does not sufficiently link this to digital surveillance. Linkage of surveillance to fundamental rights would be a positive step in making surveillance actors more accountable, since the KNCHR has a general oversight mandate for all state organs.

Issues of surveillance should receive more attention in Parliament. Parliamentary committees on security should provide reports on emerging issues including procurement of surveillance systems. For such oversight to be meaningful, parliamentarians' capacity on issues of surveillance should be built. Researchers and civil society organisations working on surveillance and human rights should therefore disseminate their research findings to parliamentarians, who could serve as a useful mechanism for seeking

information on surveillance programmes. Parliament could also contribute to transparency, and provide oversight and accountability.

Lack of transparency is a problem. Mandatory SIM card registration, for example, has been faulted by several civil society organisations. During Kenya's 2019 universal periodic review by UN mechanisms, mandatory SIM registrations were linked with surveillance of human rights defenders (UPR Info 2020). Whereas national security is used as a reason for requiring registration of the SIM cards, registration has been cited as providing law enforcement officers direct access to telecommunications networks. Networks do not publish information on government requests for such access (*ibid.*).

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

- Surveillance systems such as hate speech monitoring and anti-corruption are implemented in a legal vacuum, contrary to the guidance of the UN Draft Legal Instrument. Kenya should enact a specific surveillance law prior to purchasing or developing surveillance systems. The law should cover both surveillance systems and use of non-surveillance systems such as digital ID for surveillance purposes. As surveillance is a limitation on human rights, the surveillance law should adhere to the constitutional requirement for legality, necessity and proportionality.
- While Kenya currently has a system for judicial authorisation for some types of surveillance, the system is still lacking in that there is no independent oversight body to supervise surveillance practice. Mechanisms for public accountability, such as transparency reports, are also lacking.
- Existing – and future – surveillance systems should undergo human rights impact analysis. All surveillance actors should develop mitigation measures for the people whose rights surveillance systems affect. Measures could include notification of surveillance subjects, removal from surveillance and independent review of surveillance activities.
- The law should adopt surveillance principles in the UN Draft Legal Instrument, especially on transparency of surveillance and accountability of surveillance actors. Issues requiring transparency include notification of surveillance subjects as well as publication of surveillance reports. Issues of accountability include retirement of surveillance data, so that surveillance subjects are not perpetually in government files. Similarly, health surveillance data collected during the Covid-19 pandemic should be retired once the pandemic is over.
- There should be greater protection of special interest groups such as children and people with HIV or AIDS. Mass surveillance of such groups should be specifically outlawed; and where surveillance is applied for, the requesting authority should be required to indicate to the judge whether the subject is from a protected category.
- The National Security Council should provide information on the nature of surveillance in Kenya, actors, statistics on surveillance activities and their value. In tandem, private companies involved in

surveillance such as telecommunications network operators should publish periodic reports on government surveillance requests.

- Information on health surveillance during the Covid-19 pandemic should be published. People who accessed the information as part of the pandemic response – for example, app developers – should also be required to retire that data or at least de-identify it to protect the privacy of the public.
- The NPS Act should have narrower provisions on surveillance to meet the legitimate aims and reasonable grounds recommended by international law. These should include the basis for surveillance, types of crimes that attract surveillance as well as internal and independent external oversight on surveillance activities.
- Surveillance carried out under other laws such as the Anti-Corruption and Economic Crimes Act, Kenya Revenue Authority Act, and National Cohesion and Integration Act should be contested for their lack of legitimate aims and accountability.
- All surveillance laws should have a reporting mechanism whereby Parliament and the public are made aware of the statistics, nature and value of surveillance in a given period. Subjects of surveillance should also be notified of surveillance even if this is after the fact.

Who needs more capacity to do what? Journalists, academics, researchers

- The KNCHR should extend its monitoring to surveillance activities of the various government and private bodies.
- Security researchers should be sensitised on human rights aspects of surveillance for groups such as children and people with HIV or AIDS.
- More awareness should be created about the impact of digital surveillance among the public, in general, and groups such as human rights defenders and journalists, in particular.

What additional research is needed into which areas?

- More research is needed on the impact of surveillance on groups. How can group rights impact assessments be done? How can mechanisms such as the UN Draft Legal Instrument incorporate group rights and, where groups' rights are affected, impose higher sanctions?

References

African Union (1981) ***African Charter on Human and Peoples' Rights*** (accessed 4 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)

Amoth, P. (2021) ***Guide on the Digital Verification of COVID-19 Certificates,*** Pretoria: Ministry of Health (accessed 4 August 2021)

Article 19 Eastern Africa (2020) ***'Kenya: Intellectual Property Bill Must Not Water Down Freedom of Expression Protections'***, Article 19, 5 June (accessed 10 August 2021)

Article 19 Eastern Africa; the Kenya ICT Action Network and Pollicy (2021) ***Unseen Eyes, Unheard Stories: Surveillance, Data Protection, and Freedom of Expression in Kenya and Uganda During COVID-19***, Article 19 (accessed 4 August 2021)

Boinett, B.W. (2009) **'The Origins of the Intelligence System of Kenya'**, in S. Africa and J. Kwadjo (eds), *Changing Intelligence Dynamics in Africa,* Birmingham: Global Facilitation Network for Security Sector Reform (accessed 18 September 2021)

Breckenridge, K. (2019) **'The Failure of the "Single Source of Truth About Kenyans": The NDRS, Collateral Mysteries and the Safaricom Monopoly'**, *African Studies* 78.1: 91–111 (accessed 18 September 2021)

Burt, C. (2018) ***'Kenyan Police Launch Facial Recognition on Urban CCTV Network'***, BiometricUpdate.com, 24 September (accessed 21 June 2021)

CIPESA (2019) ***Digital Rights in Africa: Challenges and Policy Options***, Kampala: Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (accessed 30 June 2021)

Communications Authority (2018) **Press Statement by Mr Francis W Wangusi, Director General, Communications Authority of Kenya (CA), on Misleading Media Reports Regarding the Regulatory Tool for Curbing Counterfeit Devices on Mobile Networks** (accessed 29 July 2021)

Communications Authority (2016) ***Tender Advert for Design, Supply, Delivery, Installation, Testing, Commissioning and Maintenance of a Device Management System (DMS)***, Nairobi: Communications Authority of Kenya (accessed 31 July 2021)

Communications Authority and National Cohesion and Integration Commission (NCIC) (2017) ***Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content Via Electronic Networks*** (accessed 30 June 2021)

eKLR (2020a) ***Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others*** (accessed 21 June 2021)

eKLR (2020b) ***Nubian Rights Forum and 2 others v Attorney-General and 6 others; Child Welfare Society and 8 others (Interested Parties)*** (accessed 13 August 2021)

eKLR (2016) ***Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others*** (accessed 13 August 2021)

East African Community (EAC) (2008) ***Draft EAC Legal Framework for Cyberlaws***, UNCTAD and EAC (accessed 10 August 2021)

eKLR (2015) ***Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya &10 others*** (accessed 13 August 2021)

Google (2021) **Government Requests to Remove Content – Kenya** (accessed 13 August 2021)

Kapiyo, V. and Githaiga, G. (2014) **'Is Surveillance a Panacea to Kenya's Security Threats?'**, in *Communications Surveillance in the Digital Age,* Global Information Society Watch (accessed 21 June 2021)

Kenyatta, U. (2020) ***Annual Report to Parliament on the State of National Security. Statutory report. Parliament of Kenya***, Nairobi: Republic of Kenya, Executive Office of the President (accessed 21 June 2021)

Lind, J.; Mutahi, P. and Oosterom, M. (2015) ***Addressing and Mitigating Violence. Tangled Ties: Al-Shabaab and Political Volatility in Kenya***, IDS Evidence Report 130, Brighton: Institute of Development Studies (accessed 10 August 2021)

Ministry of Education (2017) ***NEMIS User Guide***, Nairobi: Ministry of Education (accessed 10 August 2021)

Ministry of Interior and Coordination of National Government (2019) ***Public Participation on National CCTV Policy*** Nairobi: Ministry of Interior and Coordination of National Government (accessed 21 June 2021)

Muchunguh, D. (2021) **'DCI to Keep Records of Students Involved in Crime'**, *Daily Nation,* 26 January (accessed 26 January 2021)

Mutai, E. (2020) **'State Releases Sh1.5bn for Safaricom's Police Cameras Deal'**, *Business Daily,* 29 June (accessed 21 June 2021)

Mutung'u, G. (2018) ***The Influence Industry. Data and Digital Election Campaigning in Kenya***, Policy Paper, Tactical Technology Collective (accessed 4 August 2021)

Ng'ang'a, G. (2020) **'Security Organs Could Have Say on Harambees'**, *The Standard,* 19 October (accessed 4 August 2021)

Nyabola, N. (2020) **'Cambridge Analytica and the End of Elections'**, *Al Jazeera*, 18 January (accessed 30 June 2021)

Odhiambo, M. (2020) **'Sh40bn Allocated to Corona Response – Treasury CS Yatani'**, *The Star,* 22 April (accessed 30 June 2021)

Oketch, A. (2021) **'Kenya: Covid-19 Contact Tracing Made Easy By Tech'**, *Daily Nation*, 17 January (accessed 30 June 2021)

Olewe, D. (2020) **'Coronavirus in Africa: Whipping, Shooting and Snooping'**, BBC News, 9 April (accessed 4 August 2021)

Ombati, C. (2020) **'NIS to Lead in War Against Cartel Capture in Public Service – BBI'**, *The Standard,* 26 October (accessed 4 August 2021)

Otieno, R. and Obala, R. (2020) **'"I'll Make No Pact With Evildoers Nor Show Mercy to the Corrupt"'**, *The Standard*, 15 January (accessed 4 August 2021)

Phillips, T. (2021) **'Kenya to Combine Cashless Payments With Covid Contact Tracing on Matatu Minibuses'**, NFCW, 11 January (accessed 30 June 2021)

Privacy International (2017) ***Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya***, London: Privacy International (accessed 21 June 2021)

Republic of Kenya (2015) ***Kenya Information and Communications (Registration of SIM-Cards) Regulations, Legal Notice No 163 of 2015***, Nairobi: Communications Authority of Kenya (accessed 10 August 2021)

Safaricom (2019) **Safaricom Data Privacy Statement** (accessed 4 August 2021)

The Nation (2011) **'NCIC Monitoring SMS, Web Chatter for Hate Speech'**, *Daily Nation*, 5 May (accessed 30 June 2021)

The Presidency (2020) **'President Kenyatta Inaugurates the National Security Telecommunications Service'** (accessed 21 June 2021)

UPR Info (2020) **'Review on 23 January 2020 – Civil Society and Other Submissions'** (accessed 21 June 2021)

Surveillance Law in Africa: a review of six countries

Nigeria country report

Ridwan Oloyede

This report explores the surveillance landscape in Nigeria. It provides a concise review of the existing domestic laws, practices and jurisprudence relating to surveillance and privacy, while outlining the safeguards, checks and balances available and how they operate in practice. Surveillance is defined here as the 'monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future' (Electronic Frontier Foundation (EFF) 2014).

The report also examines surveillance cases that have played out in Nigerian courts and decides whether the existing surveillance practices are legal, necessary and proportionate. In addition, the report considers the efficacy of existing laws to protect privacy and limit surveillance. Nigerian surveillance law is then compared against international law, specifically against the UN Draft Legal Instrument on Government-led Surveillance and Privacy and the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2014). Recommendations are then made based on the analysis of legislation, gaps in existing policies and practices, and the need to protect Nigerians' privacy rights adequately. Finally, the report closes with recommendations to different stakeholders on improving the quality of legislation, understanding prevalent practices and responsibly implementing the law.

Introduction

State surveillance on its own is 'not inherently unlawful, especially when governments have legitimate reasons to undertake surveillance that is not rooted in a desire to enforce political repression and limit individual 'freedoms' (Feldstein 2019: 11). However, governments must ensure that while protecting national security they take care to avoid infringing on the human rights of their people (Privacy International 2014). Historically, Nigeria has had a repressive colonial and military past that encouraged state surveillance. Unfortunately, it has continued to fester even during the democratic dispensation. As a result, information capture to monitor Nigerian citizens' activities has proliferated in recent years, despite the legal right to privacy.

Nigeria is the most populous country in Africa, with a population of over 180 million people. In the past decade, the country has witnessed an increase in violent incidents that are threatening national cohesion,[1] which the government has cited as the justification for surveillance. The government was reported in April 2013 to have procured surveillance technology from Elbit Systems Limited in Israel (Johnson 2013; Ogala 2013) to 'advance the internet and computer-based gathering of Nigerian citizens' personal data' (Advox 2013). The government ignored protests by concerned civil organisations and citizens, and the lack of enabling legislation for such procurement, and went ahead regardless. More research (Marquis-Boire *et al.* 2013) conducted in the same year also revealed the government's involvement with global spyware giant FinFisher (*ibid.*: 104). A report titled 'Running in Circles: Uncovering the Clients of Cyber-espionage Firm Circles' also revealed that 'a telecom surveillance company by the name of Firm Circles [had] been helping state security apparatuses across 25 countries, including Nigeria, to spy on the communications of opposition figures, journalists, and protesters' (Al Jazeera 2020). The Nigerian government spent close to 46 billion naira (US$127.6 million) in 2017 (Budget Office of the Federation 2021) and budgeted almost 9 billion naira (US$22.8 million) in 2020 (Adegoke 2021) for surveillance-related activities or equipment.

Multiple state agencies now require fingerprint, facial capturing or other biometric[2] data for identification. No less than six government agencies maintain different biometric data points on citizens and residents at federal

1 There is the notorious threat posed by militant Islamist group Boko Haram, which has been reported to be the cause of more than 300,000 deaths, with more than 2 million people displaced in the north-eastern part of the country since 2002 when the group started its operations. In the north-west, communities have witnessed killings and kidnappings by armed groups. There have also been military actions in the south and the south-east.

2 Biometrics is the measurement and statistical analysis of people's unique physical and behavioural characteristics.

level,[3] while some state governments have also adopted resident registration programmes (Ajayi 2021). Some states have adopted closed circuit television (CCTV) cameras in public for surveillance and security (TVC News 2020). The live feeds from the cameras are observed from a command centre, ensuring real-time updates to law enforcement agencies. The Lagos State Vehicle Inspection Service uses licence plate recognition of CCTV images to monitor traffic offenders and impose sanctions on erring vehicle owners (QED 2018). The fine ticket is sent to the address of the owner of the offending vehicle. Some law enforcement agents in Lagos state reportedly now wear body cameras (Guardian 2021).

The Nigerian Senate in July 2021 approved 4.8 billion naira (US$11 million) to the Nigerian Intelligence Agency for the purchase of WhatsApp Intercept Solution and Thuraya Interception Solution, 'a communications system used for monitoring voice calls, call-related information, short message service (SMS) and data traffic, among others'. The deployment of these tools will impact end-to-end encryption for 'communication' (Iroanusi 2021). In the past year, Nigerians have used virtual private networks (VPNs) to beat the 'government's blocking of access to micro-blogging site Twitter (Arise News 2021). In June 2021, the government suspended the operation of Twitter in Nigeria. Nigerians have also relied on the use of other privacy-preserving communication tools such as Signal and Telegram (The New York Times 2021). According to the Committee to Protect Journalists, it 'found at least two companies that produce digital forensics tools – Israel-based Cellebrite and U.S.-based AccessData – operating in Nigeria' (Rozen 2019). The tools are capable of extracting information from phones and computers.

One might argue that the government needs targeted surveillance, primarily because of the sad realities of the state of insecurity in the country. However, civil society organisations and citizens generally are concerned that surveillance could be normalised and abused by authorities, especially in the absence of adequate legal protection. This concern has been confirmed repeatedly by the incidence of surveillance abuse by governments the world over. For example, in the case of Nigeria, research has shown that the procurement of surveillance equipment by the government was simply for 'political reasons, especially by the then authorities in power to monitor their adversaries and political opponents' (Ekott 2013). At the same time, others consider the Nigerian government to have the capability to 'intercept all internet activity and to invade users' privacy at will' (Dada and Tafida 2014).

3 Independent National Electoral Commission (voter card); Central Bank of Nigeria (bank verification number); Nigeria Police Force (tint permit, which allows drivers to wear tinted glasses); Federal Road Safety Commission (driver's licence); Nigeria Immigration Commission (international passport and residential permit); and National Identity Management Commission.

Against this background, this report provides a country assessment of the Nigerian government's use of state surveillance on citizens. In addressing the research questions, this report will provide a concise review under several subheadings.

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

Due to its lengthy colonial and military history, surveillance of citizens, dissents and opposition has been a recurrent theme. Article 7(3) of the Lawful Interception of Communication Regulations (LICR) specifies as legitimate aims for surveillance in Nigeria: national security; preventing or investigating crime; protecting and safeguarding the economic wellbeing of Nigeria; public emergency or safety interests; and giving effect to any international agreement Nigeria is a party to. The rise in domestic terrorism has also fuelled the case for surveillance, leading to increased spending in this area. In addition, the outbreak of the Ebola virus in 2014 and the coronavirus (Covid-19) pandemic in 2020 provided public health and emergency as a premise for health surveillance. Visitors' personal information was documented for testing and tracing. The motive is evident in the enactment of the Covid-19 Regulations 2020, under the Quarantine Act (Cap Q2 LFN 2004).

2. Which international conventions protecting privacy has Nigeria adopted?

Nigeria has ratified or adopted into domestic law a range of international conventions that guarantee its citizens' right to privacy and freedom from unwarranted surveillance, including those listed below.

a. **African Charter on the Rights and Welfare of the Child**

Article 10 of the charter guarantees African 'children's right to privacy. Accordingly, children enjoy protection of the law in relation to their communications and correspondence, which cannot be unduly interfered with. Nigeria ratified the charter in 2001.

b. **Universal Declaration of Human Rights**

Article 12 provides that no one should be subjected to arbitrary interference in relation to their privacy and correspondence. Thus, all Nigerians should enjoy legal protection against such arbitrary interference.

c. **International Covenant on Civil and Political Rights**

Article 17 of the covenant provides that individuals should enjoy protection from arbitrary and unlawful interference in their communications and correspondence.

d. **Economic Community of West African States Supplementary Act on Personal Data Protection**

The act creates a legal framework for the protection of personal data in the West Africa sub-region. Nigeria is a signatory to the act.These international instruments have emerged as international human rights norms Nigeria is committed to uphold in relation to protection of privacy. According to section 12 of the Nigerian Constitution, these instruments take effect and have the force of law in Nigeria when enacted into law by the legislature.

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

The most significant laws and draft bills enabling surveillance include those listed below.

a. **Constitution of the Federal Republic of Nigeria 1999**

Section 37 of the constitution guarantees the 'privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications'. However, section 45 restricts the application of rights 'in the interest of defence, public safety, public order, public morality or public health'. Nonetheless, such derogation must be 'reasonably justifiable in a democratic society'.

b. **Cybercrimes (Prohibition, Prevention, etc.) Act 2015**

Section 45(2) (e) and (f) permit law enforcement officers to apply to a judge *ex parte*[4] for a warrant to 'search any data contained in or available to any computer system or computer network' and to 'use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format'. These provisions provide one of the bases for the decryption of encrypted communication in Nigeria.

Similarly, section 38(1) of the act mandates service providers to retain traffic and content data for two years. Further, section 38(2) of the act allows law enforcement agents to request data from service providers, and they are mandated to comply. Section 38(4) prescribes that data obtained under the provision can only be used for a legitimate purpose. However, the act fails to define what constitutes a legitimate purpose. Section 45 of the act enables a law enforcement officer to apply to a judge to obtain electronic evidence in the investigation of crime without notifying the individual subject to the investigation. There is no publicly available repository or report to the legislature documenting such requests and approvals. Section 12 criminalises unlawful interception of communication with an imprisonment term of up to two years, a fine of 5 million naira (US$13,888) or both, which is consistent with the international principle on safeguards against illegitimate access. Finally, section 38(5)

4 *Ex parte* means a legal proceeding brought by one party in the absence of and without representation of or notification to another party.

prescribes that the exercise of the power must uphold the right to privacy guaranteed under the constitution.

c. **Mutual Assistance in Criminal Matters Act 2019**

Part V of the act provides for interception of telecommunications and postal items and surveillance, including covert electronic surveillance. Among other things, it allows for the exchange with other countries of: surveillance information relating to the identification and location of criminal offenders; obtaining evidence; securing the production of official or judicial records; interception of postal orders; interception of telecommunications; and conversion of electronic surveillance. An interception under the act is limited to criminal matters of a serious nature. In this regard, the government can be involved in the surveillance of citizens once it pursues a criminal investigation. The act further encourages transparency through the requirement that government requests for citizens' data should be published: such a request can only be made based on reasonable suspicion, and it must specify the purpose, the type of communication to be intercepted, the details of the recipient of the data and details of the authority concerned. The attorney general of Nigeria is designated as the central authority responsible for handling requests for mutual assistance between the countries.

d. **Terrorism Prevention Amendment Act 2013**

The act amends the Terrorism (Prevention) Act of 2011 (TPA). It gives the relevant law enforcement agency power to intercept communications to prevent terrorist acts and detect offences related to them. However, this is subject to getting the approval of the attorney general, inspector general of police and coordinator of national security. Section 29 of the act empowers the relevant law enforcement agency to conduct intelligence gathering 'for the prevention of terrorist acts or to enhance the detection of offences related to the preparation of a terrorist act or the prosecution of offenders under this Act.' The judge's order can permit the installation of a device to intercept communication. However, the order must specify the duration for the service provider to retain the communication data. Section 24 permits terrorism investigation with a judge's approval; the warrant request must specify the purpose and material relevance to the investigation. In contrast, section 25 allows an investigation without a warrant when there is a verifiable urgency, where life is threatened and when seeking the judge's approval would delay or be prejudicial to public safety. Such an officer cannot be less than the rank of the chief superintendent of police.

e. Nigeria Data Protection Regulation 2019

The National Information Technology Development Agency (NITDA) published the regulation in 2019. It creates a set of obligations for both public and private entities. The regulation provides for data protection rights, principles and lawful bases for processing personal data. Prominently, public interest exercised by public authority and lawful obligation is part of the lawful bases recognised under the regulation. The Data Protection Implementation Framework, which is an addendum to the regulation, includes processing carried out by public agencies to investigate crime, national interest and public safety as exceptions to the application of the Nigeria Data Protection Regulation (NDPR). Finally, individuals have the right to approach the court to seek redress for violation of their rights.

f. Nigerian Communications Commission Act 2003

The Nigeria Communications Commission (NCC) regulates internet service providers and mobile phone companies. The Nigerian Communications Act provides a 'regulatory framework for the Nigerian telecommunications industry'. Section 147 gives the NCC the power to determine that a licensee or class of licensee has 'the capability to allow authorised interception of communications'. Section 148 gives the NCC the power on the occurrence of 'a public emergency or in the interest of public safety' to: suspend operation licenses; take temporary control of services or network facilities; order the disclosure, interception or prevention of specified communications; withdraw services or network facilities; or order the possession of 'network facilities, service, or customer equipment' (section 148(1a–d)).

It is disturbing that the act refers to the preservation of 'national security' and dedicates sections 146–149 to 'national interest matters' but fails to provide a working definition of the terms. Section 157, which is the interpretation section, also categorically fails to spell out what qualifies as a public emergency and to define what constitutes public safety. All these provide gaps that could occasionally be abused by a future government, which could use this imprecision to curtail citizens' rights.

Outside the principal act, the NCC is empowered to issue secondary legislation to regulate the telecommunications sector. The NCC has exercised this power by issuing regulations, guidelines and a code of practice that impose an obligation on service providers to intercept communications, decrypt encrypted communication, disclose communications data to law enforcement agencies and potentially violate the right to privacy. Concerning surveillance, some of the related regulations issued by the NCC are listed below.

g. **Nigerian Communications Commission (Registration of Service Telephone Subscribers) Regulations 2011**

Part 2 of the regulation establishes the obligation to maintain a central database domiciled within the NCC for the central processing and storage of subscribers' information. Article 8 of the regulation provides for access to subscriber information on the central database by security agencies. However, it requires that a prior written request specifying the purpose of the request should be made to the NCC from 'an official of the requesting security agency who is not below the rank of an Assistant Commissioner of Police or a coordinate rank in any other security agency'.

h. **Nigerian Communications (Enforcement Process, etc.) Regulations 2019**

The regulation gives the NCC monitoring and enforcement powers. Regulation 8(1) prescribes that 'every licensee shall keep records of call data under the Cybercrimes Act and the consumer code of practice regulations'. It also requires every licensee to make available 'basic' and 'non-basic' information that may be required by law enforcement agency under section 146 of the Nigerian Communications Act (Regulation 8(2)(a, b)). It states that, concerning basic information, 'a written request from the relevant authority, duly signed by a police officer not below the rank of assistant commissioner of police or its equivalent' would suffice without any further assurance; while for non-basic information, a court order is necessary.

i. **Guideline for the Provision of Internet Service 2013**

The guidelines apply to all internet service providers (ISPs) in Nigeria. Paragraph 6 of the guidelines mandate ISPs to cooperate with 'all law enforcement and regulatory agencies investigating cybercrime or other illegal activity'. In addition, ISPs must provide investigating authorities with service-related information, information about users, and the content of their communication. Paragraph 8 of the guidelines mandates ISPs to retain user identification, content of user message and traffic data for twelve months. The power to intercept communication data is not subject to an independent oversight.

j. **Registration of Telephone Subscribers Regulation 2011**

The regulation makes it mandatory to for subscribers to register SIM cards with their biometric data and also establishes a central database of all registered subscribers in the country. The provision legitimises mandatory SIM registration in the country, which erodes anonymity. Article 9 of the regulation guarantees the privacy and confidentiality of subscriber information. However, the data can be accessed by security agencies if a request is made to the NCC by an officer not below the cadre of an

Assistant Commissioner of Police (art. 8). The request must specify the reason the information is required. In what appears to be a safeguard, article 10 of the regulation specifies that the release of subscribers' personal information to security agents must comply with existing law, and such a request can be refused if it constitutes a breach of the constitutional provision or any other law or is a threat to national security.

k. Lawful Interception of Communications Regulations 2019

The scope of the regulation includes the provision of a 'legal and regulatory framework for lawful interception of communications, collection and disclosure of intercepted communications in Nigeria'. It stipulates that only an authorised agency may affect the interception of communications. It gives these powers only to the Department of State Security, the Nigeria Police Force and the Office of the National Security Advisor, subject to obtaining a court warrant. The warrant to intercept can be granted when interception is the only way to access the communication data and if the 'facts alleged in the application are reasonable and persuasive enough' to provide sufficient evidence that the surveillance subject has or is about to threaten a legitimate aim (LICR art. 13(3)).

Article 9 gives the authorised agency the power to request protected or encrypted communications disclosure. Security officers have been enabled to intercept phone calls, text messages, chat messages or emails on this premise (Collins 2013). However, the authorised agency must submit an annual report of all concluded interception cases to the attorney general. The report is not made publicly available. It allows the authorised agency the liberty to store intercepted communications for the duration of its investigation. Article 10 mandates service providers to install interception capabilities that permit interception. Similarly, article 11 prohibits network providers from providing services that cannot be intercepted and monitored. An application for a warrant should include the duration, the grounds for the application, the identity of the subject of interception, and the investigating authority's identity. Article 5 makes it an offence to unlawfully intercept communication, which is consistent with the international principle of imposing safeguards against illegitimate access.

Article 7 provides for an interception with a warrant, while article 8 allows interception without a warrant. When interception is carried out without a warrant, the investigating authority must apply for a warrant to a judge of the Federal High Court within 48 hours after the interception has occurred. Where the application is not made, the interception shall terminate and be treated as unlawful. Similarly, article 13(2)(d) of the LICR provides that

where the judge rejects an application for the interception that has taken place, any information obtained before the refusal is invalid and not admissible for criminal persecution of the individual affected by it. The information extracted is valid for the investigation period and destroyed after the conclusion of the investigation. In addition, the information is confidential and can only be used for investigation and prosecution in a criminal proceeding. An interception order granted by a judge is valid for three months or a lesser period specified by the judge, after which the record can be archived for three years and destroyed afterwards.

Interestingly, article 20(1) of the LICR allows a network provider or any individual aggrieved about any interception activity to notify the NCC or make a formal application to the Federal High Court for judicial review. Unfortunately, it may be difficult for individuals to know they have been targeted for surveillance if they are not notified about it. Specifically, article 13(4) of the LICR provides that an application for a warrant shall be heard without placing the individual affected under notice.

Other laws and proposed bills

The National Security Agencies Act is another critical piece of legislation, which established the State Security Service, Defence Intelligence Agency and National Intelligence Agency, the government agencies responsible for intelligence gathering in different capacities in the country. There have also been legislative proposals to legitimise surveillance by the legislature. The Telecommunications Facilities (Lawful Interception of Information) Bill 2019 seeks to compel telecommunications service providers to enable law enforcement agents to intercept communications for national security purposes. Section 3 of the bill requires service providers to hand over intercepted communications to law enforcement agents. The provision also allows the decryption of communications. Section 13 mandates network providers to hand over subscribers' personal information to law enforcement agents. Any appeal over violation of the law goes to the minister of justice. The bill is currently at its first reading in the House of Representatives (lower federal legislature).

The Digital Rights and Freedom Bill 2019 provides for online privacy rights and defines the legal framework regarding surveillance. The bill outlines the provisions of lawful and authorised interception of communication within the digital environment. It grants the court more powers to perform oversight functions. Under the bill, surveillance is made subject to necessity and furtherance of a legitimate aim. In stemming the asymmetrical power dynamics between law enforcement and private citizens, the bill

proposes that private organisations make public the details of government requests for private citizens' data. The bill is currently awaiting the House of Representative committee report.

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

Some African countries have been reported to engage in arbitrary mass surveillance (Citizen Lab 2020). In addition, there are fears that several governments are procuring surveillance tools to monitor dissidents, political opponents, human rights defenders and journalists. Algeria, Botswana, Côte d'Ivoire, Egypt, Ghana, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia and Zimbabwe were recently reported to have procured and deployed surveillance tools (Jili 2020). In July 2021, after a forensic investigation, the Guardian and other media outlets reported the use by some African countries such as Rwanda, Togo, and Morocco of Israeli company NSO Group's malware, Pegasus, which allows security agencies to listen to phone calls, intercept messages, and also to track individuals (Damien 2021). The malware has been reportedly used to spy on dissidents, opposition, journalists, and foreign leaders (Lynsey 2021). Although Rwandan and Moroccan governments have denied the claim (Kirchgaessner 2021, Shaquile 2021), in 2019, dissident and human rights activists from Rwanda and Morocco were privately warned by communication giant WhatsApp that they were victims of cyber-attacks designed to infiltrate their phones by an NSO Group malware (Kirchgaessner *et al.* 2019).

The pervasive practice appears to go unchallenged due to vague laws that are subject to abuse, codification of state power to conduct mass monitoring, the absence of independent oversight bodies, and weak legal frameworks and institutions. For example, in Uganda, facial recognition has been deployed to monitor protesters (Quartz Africa 2020b).

Nonetheless, there are examples of progressive practices on the continent. In South Africa, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) is the primary law on surveillance. The RICA creates an oversight body and puts in place several safeguards contained under the International Principles. However, the law also omits some safeguards. The legal frameworks in South Africa and Nigeria lack safeguards on transparency. There is no statutory requirement to publish a public annual report, although in Nigeria a report is meant to be submitted to the attorney general. Both countries omit the obligation to notify individuals either before they are surveilled or at the conclusion of surveillance. Under Nigeria's Cybercrimes Act, investigating authorities can apply to the court to conduct surveillance without notifying the individual

being surveilled and there is no avenue to challenge the surveillance measure or appeal the decision. Both the RICA and LICR mandate the communication service provider to ensure their communication tools are capable of being intercepted, which is contrary to the international principle of integrity of communications and systems and could also open a floodgate for unregulated surveillance.

Both countries have a requirement to specify the category of offence before requesting a judicial directive. The TPA requires specifying the subject of surveillance in the application to the judge. There also appears to be a normative condition to establish a legitimate aim before surveillance. The South African law also has the benefit of being tested before the court. For example, in 2021 South Africa's Constitutional Court delivered a landmark judgment outlawing mass surveillance in the country. In *Amabhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services (CCT 278/19)* the court held that the government should no longer conduct mass surveillance of citizens. The court also declared certain parts of the RICA unconstitutional (BusinessTech 2021). Notably, the court stated that the RICA fails to provide sufficient safeguards to preserve the right to privacy, the law did not provide adequate protection or relief for persons subjected to surveillance, and the law did not make provision for individuals subjected to surveillance to be notified after the fact, among other issues. Nevertheless, South Africa has a specific surveillance law, as recommended by the UN Draft Instrument, while in Nigeria legal surveillance provisions are located in different laws. This could be considered preferable to having contradictory legitimate aims and safeguards specified in different pieces of legislation, as in Nigeria. South Africa has a more explicit definition of tests for a judge to assess before issuing authorisation, which is not evident in all cases in the Nigerian framework. South Africa has an 'independent oversight board' as conceptualised under the International Principles. The law in South Africa also has the advantage of being challenged and tested in court by civil society in ways that have identified flaws, clarified provisions and provided enhanced privacy protections.

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

The UN Draft Legal Instrument on Government-led Surveillance and Privacy sets out principles and safeguards on the minimum requirements to conduct surveillance. Article 4 of the UN Draft Legal Instrument sets out the principles. A quick review of the Nigerian legal framework – including the Mutual Legal Assistance Act and the TPA – suggest appreciable adherence to the requirement for a legitimate aim, such as the interception for serious crimes. In addition, the Nigerian framework requires specifying the details to be intercepted in the application for warrant and only intercepting when there is a reasonable suspicion and interception is the only way to access the communication data, which suggests necessity. There are other additional safeguards. For example, under the LICR, the failure to obtain a warrant where it is required renders the evidence unlawful and unacceptable before the court.

An appraisal of existing Nigerian laws against other principles shows a contrasting picture for some parts. Nigeria's laws are noticeably lacking in sufficient procedural safeguards and an independent oversight mechanism of the activities of investigating authorities. The UN Draft Legal Instrument recommends that government or police officials should seek prior authorisation for surveillance from a court and that an oversight body independent of both the court and government or police be given the power to access all requests and authorisations to ensure that robust checks for the legality, necessity and proportionality of surveillance are implemented, and that notification is provided to the individuals under surveillance. Specifically, the LICR makes it mandatory not to notify the subjects of surveillance when the investigating authority is applying to the court for a warrant to intercept communication, which deprives the individuals concerned of the right to an effective remedy. Notification is essential to fight surveillance overreach. Although the LICR allows individuals who are subject to surveillance to approach the NCC or Federal High Court for judicial review if dissatisfied (LICR, art. 20), the mandatory requirement not to notify them robs them of the chance to be aware of the interception before or after the fact (LICR, art. 13(4)).

Both the TPA and LICR mandate network service providers to install tools that can enable interception capability, which is contrary to the principle of integrity of communications under the UN Draft Legal Instrument. The failure

to install the tool is punishable with a fine or withdrawal of operation license. Also, the LICR permits interception for 'investigation of crime' and fails to make a distinction or allow interception for the most severe crimes, which could allow the abuse of investigative powers. The Nigerian law also includes the notification to the regulator and the data subjects when there is a data breach.

Another principle of the UN Draft Legal Instrument is the requirement to ensure safeguards by law enforcement agencies. For example, the LICR and the Cybercrimes Act suggest that the application for a warrant should specify the subject of the interception and the grounds on which the application is being made, which is consistent with the requirement of reasonable suspicion. Under the LICR, the obligation to ensure the security of the transmission of data is placed on the network provider. The intercepting agency must ensure data are stored confidentially, which is consistent with the principle of ensuring confidentiality and integrity of communications data under the UN Draft Legal Instrument. Similarly, other laws, such as the NDPR, impose security obligations on public agencies.

Another requirement addresses intelligence sharing with other countries. The UN Draft Legal Instrument favours a regime where independent and cross-border data transfer rules are adequate. However, under the Mutual Legal Assistance Act, the attorney general, a political appointee of the government, is responsible for exercising this power in Nigeria. In addition, the LICR mandatory requirement for installation of surveillance capability and decryption of encrypted communication could pave the way for unregulated bulk data collection, contrary to one of the principles in the UN Draft Legal Instrument. Also, there are instances of the government deploying surveillance tools, as highlighted in the introduction of this report, but there is no record or evidence of a human rights impact assessment being conducted. None of the laws on surveillance in Nigeria makes it mandatory to conduct a human rights impact assessment. Finally, transparency about requests and authorisations through the publication of an annual report is only visible under the LICR. The report is meant to be submitted to the attorney general and it is not made public.

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

Generally, not all laws define these phrases. The TPA sets out prevention of terrorism as its legitimate aim. Under some laws, such as the Mutual Legal Assistance Act and the TPA, it is a requirement to specify the purpose of interception. Similarly, these laws require that the application for an interception should include the scope and scale of communication data required. The provisions appear to prohibit mass surveillance. Also, section 45(3) of the Cybercrimes Act specifies that a warrant to decrypt data will only be issued where there is suspicion that the person named in the warrant is about to commit a crime. The exercise of the power is not reserved for the most severe crimes. The legitimate aim under the TPA is prevention of terrorism; whereas the Mutual Legal Assistance Act applies to the most severe crimes. The TPA allows intelligence gathering without a warrant where there is an emergency. However, it fails to define what constitutes an emergency and that imprecision could be abused.

Under the Implementation Framework to the NDPR, and the Nigerian constitution, the rights guaranteed can only be derogated in limited circumstances prescribed by law. The Supreme Court in the case of *Military Governor of Lagos State v. Ojukwu (2001) FWLR (Part 50) 1779,* held that:

> the Nigerian Constitution is founded on the rule of law, the primary meaning of which must be done according to the law. It also means that government should be conducted within the framework of recognised rules and principles which restricts discretionary powers.

The derogation to the right to privacy under section 45(1)(a) of the constitution specifies that it has to be 'reasonably justified in a democratic society'. Consequently, surveillance is not expected to be used arbitrarily.

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

Section 45 of the Cybercrimes Act and article 17 of the LICR require an interception application be made to a judge. However, there is no evidence to suggest if there is recourse to a court, considering that it is done without notifying the individual subject of surveillance. In many cases, the individual is only aware of surveillance if there is an arrest based on a request for communication data from a network provider or in a criminal prosecution if it becomes part of the evidence. In 2018, a journalist, Samuel Ogundipe, was arrested by the police using communication data obtained from a network service provider. Samuel's arrest is not an isolated case; the Committee to Protect Journalists profiled other cases where journalists were arrested by the police using records from their network provider (Jonathan 2020). There are also reported instances of journalists' phones, computers and other devices being seized by authorities to conduct forensic searches to establish their sources of information (Jonathan 2019). In another instance, a Twitter user that created a parody account in the name of former president Goodluck Jonathan was arrested by the police and detained for 54 days by obtaining call records from a network service provider (Sahara Reporters 2020). The pattern suggests surveillance is being used arbitrarily for just any crime at the behest of security agents, and there is a disregard for rule of law and legal safeguards.

The LICR and the Mutual Legal Assistance Act designate the attorney general as the central authority concerning international mutual assistance. The LICR specifies that surveillance data collected should not be kept longer than necessary and should be destroyed afterwards. The same regulation stipulates a limit of three years for the retention of data. Similarly, the Cybercrimes Act prescribes two years as the limit to retain traffic data, while the Guidelines for the Provision of Internet Service prescribes a limit of twelve months Arbitrary retention of data deprives people of anonymity. According to EFF (Electronic Frontier Foundation 2021):

> Government mandated data retention impacts millions of ordinary users compromising online anonymity which is crucial for whistle-blowers, investigators, journalists, and those engaging in political speech. National data retention laws are invasive, costly, and damage the right to privacy and free expression. They compel ISPs and telcos to create large databases of information about who communicates with whom via Internet or phone, the duration of the exchange, and the users' location.

The institutional mechanism to ensure checks and balances is almost non-existent. There is no independent oversight body to monitor activities of investigating authorities. The role of the Federal High Court is limited to surveillance requests brought to its attention. There is no similar provision to request an audit or to publicly publish a transparency report of authorisations and interception requests. Although the LICR makes it a requirement for law enforcement agencies to submit a report to the attorney general, there is no way to verify if this is observed in practice. The provision that seems to have paved the way for accountability, the transparency report, is meant to be presented to the attorney general, a political appointee, who is not an independent authority. It is instructive to say that Nigeria has an access to information law, the Freedom of Information Act.

There is also no obligation for organisations to publish a transparency report on the number and types of requests they get from the government. The Digital Rights and Freedom Bill makes it a requirement to publish a transparency report stating the types of request made by the government. To get an idea of the extent and types of requests made by the Nigerian government, one may look at the transparency report published by big technology companies. It is hard to independently verify the practical application of and adherence to these principles because surveillance is shrouded in secrecy (Dada and Tafida 2014). Also, the role of research and disclosures by entities selling surveillance tools has provided insights into the government's capability (Citizen Lab 2020). Finally, none of the laws makes it a requirement to conduct a human rights impact assessment before deployment of surveillance tools by the government.

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

The Nigerian court has recognised the right to privacy and data protection. Data protection rights available to individuals are contained under the NDPR. However, public authorities could use derogations in areas such as public interest, national security and investigation of crime to limit the exercise of those rights. The constitutional guarantee of the right to privacy is also limited in similar circumstances and when it would affect the rights of another individual. This is a common scenario with many regulations: they broadly provide for a right, then list wide-ranging exceptions that derogate from the right that seeks to be protected. The efficacy of existing privacy laws is affected by the inadequate regulatory framework surrounding privacy protection in Nigeria. Nigeria lacks a comprehensive data protection law and an independent data protection authority to enforce the law. The gaps in laws and practices have been consistently exploited by authorities to violate the privacy rights of Nigerian citizens, civil society and the media (Adegoke 2021).

The laws enabling surveillance impose obligations to preserve the right to privacy guaranteed under the constitution, but government agencies are known for violating this right. For example, the NITDA issued a notice of enforcement on the Nigeria Immigration Service for violating a citizen's privacy by publishing their biodata on social media platform Twitter, but they failed to issue a sanction or disclose the outcome of the investigation (Umoren 2019). Measures adopted by the government cast doubt on the intention to preserve privacy. The enactment of a law allowing the decryption of encrypted communication, the requirement on network providers to install interception capability, the requirement for mandatory registration of SIM cards for mobile devices, the forced integration of SIM registration with the national biometric identity number, and evidence of procurement of surveillance tools do not suggest the intention to preserve privacy. Surveillance is shrouded in secrecy and it is often hard to know which law is being relied upon.

However, section 26(3) of the National Identity Management Commission (NIMC) Act 2007 allows the information of an individual to be given without the individual's consent if it is 'in the interest of national security; necessary for purposes connected with the prevention or detection of crime; or for any other purpose as may be specified by the Commission in a regulation.' The

problem with this provision is that the terminologies are not defined; and simply throwing around the defence of national security or public interest without a qualified, legitimate purpose would only occasion arbitrary restriction of citizens' rights. States must instead 'demonstrate the risk that a specific expression poses to a defined national security or public order interest' (United Nations General Assembly 2014) and show that it is in the interest of the whole nation, and not just 'the sole interest of a Government, regime or power group' (Office of the High Commissioner for Human Rights 2019).

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

The constitutional guarantee of the right to privacy can only be derogated in limited circumstances. Safeguards should ensure that any such interceptions are legal, necessary and proportionate. The comparative assessment in this report suggests that existing surveillance law and practices in Nigeria do not entirely meet the legal threshold. Although surveillance is founded in law, it is hard to know which laws enforcement agencies rely upon in practice. A case in hand is the procurement of surveillance tools by some governors in the south of the country. The tools were acquired mainly to spy on political opponents (Ogala 2016). Presumably, all of this happened outside of the law and without the authorisation of the court.

Article 13(3)(b) of the LICR specifies that a judge should only grant a warrant where 'interception of such communication is the only means of obtaining the information required' and if the 'facts alleged in the application are reasonable and persuasive enough' to provide sufficient evidence that the surveillance subject has or is about to threaten a legitimate aim. The provisions suggest the requirement of necessity. Section 39 of the Cybercrimes Act requires that interception can only be done where there is reasonable suspicion of a crime. However, tracking journalists' phones and their subsequent arrests or conducting forensic investigations on their computers does not appear to be necessary (CPJ 2019). Similarly, the retention period of data for up to two and three years under the Cybercrimes Act and the LICR, respectively, is excessive. Consequently, these extreme measures cannot be considered proportionate, but rather a violation of fundamental rights. In Nigeria, then, multiple examples of surveillance are neither legal, necessary nor proportionate. However, these failings have yet to be challenged in court.

The LICR also imposes a limit on the duration of surveillance, which should be restricted to the period of the investigation and the record should be deleted upon completion of investigation. Intercepted communication can only be used for investigation and criminal prosecution. The judge may grant a warrant for three months or for a lesser period.

10. How has surveillance law played out in court in Nigeria?

Due to the secrecy around state-sanctioned surveillance in the country, the absence of transparency about interceptions and notification of individuals under surveillance, there were no records of court decisions specifically challenging surveillance at the time of writing. However, there are number of cases that slightly impact surveillance. The Court of Appeal has recognised the right to privacy in the case of *Emerging Markets Telecommunication Services Ltd v. Godfrey Eneye (2018) LPELR-46193(CA)*. In 2013, Pan-African digital rights organisation, Paradigm Initiative, filed a freedom of information request before the Nigerian government to provide additional details about its contract with Elbit Systems to purchase surveillance tools, which was not responded to (Irene 2013). Earlier, it become public that the government awarded a US$40 million to Elbit Systems to purchase surveillance tools (Ogala 2013). Subsequently, the organisation instituted a case before the Federal High Court to mandate the government to provide more information about the contract. The court did not grant the request (Premium Times 2013).

In 2017, Paradigm Initiative filed a freedom of information request before the Ministry of Science and Technology, requesting information about the details of the proposed launch of two satellites by the National Space Development and Research Agency (NASDA) (Okunola 2017). The ministry refused to respond to the request. Consequently, the group approached the Federal High Court to direct the ministry to provide information about the satellite launch. The court granted the request of the organisation and directed the ministry to provide the information requested.[5]

In another case, Paradigm Initiative challenged the provision of section 38 of the Cybercrimes on mandatory data retention for violating the right to privacy under the constitution and other international human rights instruments Nigeria is committed to. Both the Federal High Court and the Court of Appeal ruled against the organisation. The Court of Appeal decided that the provision on data retention is necessary to assist in the detection and investigation of crime for the public good.[6] The organisation appealed the decision, and the case is currently pending at the Supreme Court at the time of writing (Paradigm Initiative 2018). Similarly, in 2019, the organisation

5 Incorporated Trustee of Paradigm Initiative for *Information Technology Development v. Ministry of Science and Technology.* FHC/CS/481/2017

6 Incorporated Trustee of Paradigm Initiative for *Information Technology Development and others v. Attorney General of the Federation.* CA/L/556/2017

sent a Freedom of Information Request to the NCC asking for information about the legal safeguards in the surveillance practices of the government after enacting the Mutual Assistance in Criminal Matters Act (Paradigm Initiative 2019). The act permitted the interception and sharing of intelligence with other countries. Also, there is an increasing number of cases going before the court founded on the violation of the right to privacy and data protection.

Regardless, there is a significant role for strategic litigation to challenge existing legal provisions that violate fundamental human rights enshrined in the constitution and international human rights norms to which Nigeria has committed. The media have a huge role in drawing attention to these laws and holding intelligence services to account. The use of the freedom of information law to test accountability and transparency could prove significant in understanding law enforcement agents' activities.

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

Some of the laws have provisions that comply with UN principles, which is commendable. However, the challenge has been the government's non-adherence to provisions of the law and the arbitrary use of state power. A noticeable gap in existing policies is the lack of a comprehensive framework that regulates the country's data protection and privacy space and the absence of an independent data protection authority. How then does a country without an exhaustive legal framework for data protection intend to monitor communications or guarantee a remedy for violations of the data protection right within the ambit of the law?

The country also lacks the needed political will to drive such exhaustive policies. For instance, the country's draft data protection bill was presented before the 6th National Assembly (2011–2015) without success. The 7th National Assembly passed the data protection bill in 2019, which President Muhammadu Buhari rejected. No reason was adduced publicly for the bill's rejection (Oloyede 2021). Rather than drive policies, budgetary spending on surveillance has increased in the past decade (Adegoke 2021). The enactment of a law allowing the decryption of encrypted communication, the requirement for mandatory registration of SIM cards and forced integration with a national biometric identity, and evidence of procurement of surveillance tools do not suggest the intention to preserve privacy. Also, the requirement on network providers to install interception capability is contrary to the principle of integrity of communications.

The increased introduction of surveillance technologies in the country without independent institutional oversight and a mandatory requirement to conduct a human rights impact assessment before using them makes it easy to subject citizens to unnecessary and disproportionate surveillance. In addition, safeguards such as the right to notification, right to effective remedy, an independent oversight regime for intelligence sharing and review and the right to appeal an assessment contained in international human rights instruments are also missing. Lastly, transparency about requests and authorisation is shrouded in secrecy.

12. What recommendations arise from this analysis for legislation, practice or further research?

For policymakers and legislators

- Existing laws should be reviewed to incorporate the principles espoused in the UN Draft Legal Instrument. The amendment should consider the following:
    - Mandatory notification of individuals to enable them to contest surveillance;
    - Institutionalising an independent oversight body to review decisions and intelligence sharing with third countries;
    - A mandatory requirement to conduct human rights and data protection impact assessments before deploying surveillance tools;
    - The right to appeal assessment; and
    - An obligation to notify the data protection authority when there is a data breach.
- Nigeria should enact a comprehensive data protection law.
- The Digital Rights and Freedom Bill should be passed and enacted into law.
- NCC regulations should be reviewed to enforce judicial oversight and to accommodate a mandatory publicly accessible annual report. Only a judge should determine legitimate purposes.
- Members of the legislature should pass a resolution demanding greater transparency about the activities of law enforcement agencies concerning requests for communications data. They should also exercise their supervisory powers guaranteed under the constitution to audit the affairs of law enforcement agencies.

For civil society organisations and activists

- There is a need for mode data-driven research to show the extent of the government's surveillance capability.
- There should be an increase in the use of freedom of information requests to demand accountability and transparency from public authorities on procurement and use of surveillance tools.

- There is a need to demand greater accountability and transparency from the government through constant engagement, using freedom of information law and exploring strategic litigation to clarify the law, narrow surveillance targets, and protect and safeguard citizens' rights.
- Civil society organisations should challenge intelligence services over violations of the laws or existing human rights instruments that Nigeria is a party to.
- Civil society organisations should raise public awareness concerning privacy and data protection rights. This would promote citizens' self-awareness concerning protection of their digital rights.
- There is an urgent need for strategic litigation to demand accountability and question the disregard for the provisions of existing laws. Also, vague words that could lead to abuse of power should be challenged before the courts.

For government

- The government should be transparent about its procurement of surveillance tools.
- Publication of details of interception requests made should be publicly available to promote transparency and accountability.
- The attorney general's office should serve the interests of the people instead of seeking to preserve the government that appointed it.
- Institutions should be adequately funded to carry out their statutory duties.

For researchers and academia

- It is recommended that a regulatory impact assessment should be conducted to highlight failures, gaps and what is currently working in the existing legal framework.
- There is a need to build additional capacity within Nigerian legal, civil society and academic research communities to more effectively monitor, map and analyse the existing characteristics of surveillance law and practice in Nigeria, which is a necessary precondition for defining effective legal and policy measures to improve the current situation.
- It is recommended that more research should be carried out to reveal new evidence on the tools, scale, methods and tactics the government uses to conduct surveillance.

For journalists

- Journalists should raise public awareness about the government's surveillance practices and their effects to build political pressure for changes in law and practice.
- There is a need to invest in capacity building of journalists to understand the implications of surveillance and its different manifestations to present the public with an informed perspective.
- More research needs to be done to understand the categories and volume of cases in which surveillance data are used as evidence.

References

Adegoke, A. (2020) ***'Digital Rights and Privacy in Nigeria'*** *Paradigm Initiative* (accessed 26 May 2021)

Adegoke, B. (2021) **'COVID-19, digital rights and Nigeria's emerging surveillance state'** *Global Voices* (accessed 26 May 2021)

Advox (2013) ***'Nigerian Government to Ramp up Internet Surveillance?'*** *Global Voices* (accessed 29 July 2021)

Ajayi, A. (2021) **'Insecurity: Oyo to Register Residents'**, *Peoples Gazette*, (accessed 18 September 2021)

Al Jazeera (2020) ***'Nigerian Intelligence Bought Tool to Spy on Citizens: Report'***, (accessed 12 May 2021)

Arise News (2021) ***'Nigerians Opt for VPNs Following Twitter Ban'*** (accessed 15 July 2021)

Billstrack (2016) ***'Digital Rights and Freedom Bill'*** (accessed 26 May 2021)

BusinessTech (2021) ***'South Africa's RICA Law Is Unconstitutional: Court Ruling'*** (accessed 31 July 2021)

Budget Office of the Federation (2021) ***'Budget Document'*** (accessed 12 May 2021)

Citizen Lab (2020) ***'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles'*** (accessed 1 July 2021)

Collins, K. (2013) ***'Nigeria embarks on a mobile phone surveillance project'*** (accessed 26 May 2021)

Committee to Protect Journalists (CPJ) (2018) ***'Nigerian Journalist Jailed for Refusing to Reveal Source'*** (accessed 26 May 2021)

Dada, J. and Tafida, T. (2014) ***'Communications surveillance in a digital age'*** (accessed 11 May 2021)

Dada, J and Tafida, T. (2014) ***'Online surveillance: Public concerns ignored in Nigeria'*** Global Information Society *Watch* (accessed 1 July 2021)

Damien G. (2021) **'Morocco, Rwanda, Togo...How Involved Is Africa in 'Pegasus Gate'?'**, *The Africa Report* (accessed 28 July 2021)

Egbunike, N. and Burbidge, D. (2013) ***Nigerian Government to Ramp Up Internet Surveillance?*** (accessed 26 May 2021)

Ehiagwina, F. (2015) ***'Managing Insecurity with Biometric Engineering: An Overview of the Nigerian Experience'***, paper presented at the International Academic Conference on Globalization and Contemporary Issues: Opportunities for Sub-Sahara African Transformation & Development (accessed 4 August 2021)

Ekott, I. (2013) **'ACN Urges Nigerians to Resist Jonathan's 'Evil' $40million Internet Spy Contract'**, *Premium Times*, 29 April (accessed 11 May 2021)

Electronic Frontier Foundation (EFF) (2021) ***'Mandatory Data Retention'*** (accessed 28 July 2021)

Electronic Frontier Foundation (EFF) (2014) ***'International Principles on the Application of Human Rights to Communications Surveillance'*** (accessed 26 May 2021)

Federation of American Scientists (2021) ***'State Security Service (SSS) – Nigeria Intelligence Agencies'*** (accessed 1 July 2021)

Feldstein, S. (2019) ***'The Global Expansion of AI Surveillance'*** *Carnegie* (accessed 26 May 2021)

Guardian (2021) **'Response from NSO and Governments'** (accessed 28 July 2021)

Irene P. (2013) ***'Paradigm Initiative Nigeria Seeks Information on Surveillance Systems in Nigeria'*** *The Citizen Lab* (accessed 28 July 2021)

Iroanusi, Q. (2021) **'Nigerian Govt Moves to Control Media, Allocates N4.8bn to Monitor WhatsApp, Phone Calls'**, *Premium Times* (accessed 15 July 2021)

Jili, B. (2020) ***'Surveillance Tech in Africa Stirs Security Concerns'*** *Africa Center for Strategic Studies* (accessed 1 July 2021)

Johnson, J. (2013) ***'Scandal in Nigeria over Israeli arms firm's Internet spying contract'***, *The Electronic Intifada* (26 May 2021)

Jonathan R (2020) ***'How Nigeria's police used telecom surveillance to lure and arrest journalists'***, *Committee to Protect Journalists* (accessed 28 July 2021)

Jonathan R. (2019) '***Nigerian Military Targeted Journalists' Phones, Computers with 'Forensic Search' for Sources'*** *Committee to Protect Journalists* (accessed 28 July 2021)

Kirchgaessner, S. (2021) **'Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance'**, *The Guardian*, (accessed 29 July 2021)

Kirchgaessner, S.; Hopkins, N. and Holmes, O. (2019) **'WhatsApp 'Hack' Is Serious Rights Violation, Say Alleged Victims'**, *The Guardian*, (accessed 29 July 2021)

Lagos State Resident Registration Agency (2020) ***'Welcome!'*** (accessed 28 May 2021)

LawNigeria (2018) ***'Constitution of the Federal Republic of Nigeria 1999 (With Amendments)'*** (accessed 26 May 2021)

LawNigeria (1999) ***'Constitution of the Federal Republic of Nigeria'*** (accessed 26 May 2021)

Lynsey C. (2021) ***'Pegasus Lands in Africa'***, *Foreign Policy* (accessed 28 July 2021)

Marquis-Boire, M. (2013) ***'For Their Eyes Only: The Commercialisation of Digital Spying'*** *The Citizen Lab* (accessed 26 May 2021)

Munis, V.O. (2014) ***'CBN Introduces Bank Verification Numbers'*** *International Law Office* (accessed 26 May 2021)

Office of the High Commissioner for Human Rights (2019) ***'Surveillance and human rights – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'*** (accessed 26 May 2021)

Ogala E. (2016) ***'Investigation: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others'***, *Premium Times,* (accessed 28 July 2021)

Ogala, E. (2013) **'Jonathan awards a $40million contract to an Israeli company to monitor computer, Internet communication by Nigerians'**, *Premium Times,* (accessed 26 May 2021)

Okunola, F. (2017) ***'Digital Rights Organization Gets Boost in Suit against the Science & Tech Ministry'*** *Pulse* (accessed 28 July 2021)

Oloyede R. (2021) ***'Legislative prediction for privacy and data protection in Nigeria'*** (accessed 15 July 2021)

Oloyede, R. (2020) ***'A comparative analysis between the Digital Rights and Freedom Bill and other legislation in Nigeria'*** (accessed 26 May 2021)

Paradigm Initiative (2019) ***'Paradigm Initiative sends FoI Request to NCC on Nigeria's New Surveillance Provisions'*** (accessed 28 July 2021)

Paradigm Initiative (2018) ***Legal Battle Over Cybercrimes Act Moves to the Supreme Court*** (accessed 28 July 2021)

Paradigm Initiative and Privacy International (2018) ***'Stakeholder Report Universal Periodic Review 31st Session'*** (accessed 26 May 2021)

Premium Times (2013) **'Judge Asks National Assembly to Restrict Application of FOI Act'** (accessed 28 July 2021)

Privacy International (2014) ***'Nigerian Government under Fire for Expansion of Surveillance Programs***' (accessed 3 June 2021)

Quartz Africa (2020a) ***Nigeria, Kenya Use Israeli Surveillance Tool to Listen to Calls*** (accessed 1 July 2021)

QED (2018) ***'We Now Use Cameras to Track Vehicles in Lagos'*** (accessed 26 May 2021)

Quartz Africa (2020b) ***'Uganda Uses China's Huawei Facial Recognition to Snare Protesters'*** (accessed 1 July 2021)

RightDocs (2017) ***'The right to privacy in the digital age'*** (accessed 26 May 2021)

Rozen, J. (2019) ***'Nigerian Military Targeted Journalists' Phones, Computers with 'Forensic Search' for Sources,*** Committee to Protect Journalists (accessed 20 May 2021)

Sahara Reporters (2020) ***'How Ex-Nigerian President, Goodluck Jonathan, Got University Student Who Created Parody Twitter Account in His Name Detained for 54 Days'*** (accessed 28 July 2021)

Salau, G. and Akomolafe, J. (2021) **'Lagos Kits LASTMA, VIO, Others with Body Cameras to Check Abuse, Crime'**, *The Guardian* (accessed 28 May 2021)

Sesan, G.; Soremi, B. and Oluwafemi, B. (2013) ***'Economic Cost of Cybercrime in Nigeria'*** (accessed 26 May 2021)

Shaquile G. (2021) **'Pegasus Project: Morocco's Public Prosecutor Orders Probe into 'False Allegations''**, *Morocco World News*, (accessed 29 July 2021)

The New York Times (2021) **'Millions Flock to Telegram and Signal as Fears Grow over Big Tech'** (accessed 15 July 2021)

Tukur, S. (2017) **'Shocking Revelation: 100,000 Killed, Two Million Displaced by Boko Haram Insurgency, Borno Governor Says'**, *Premium Times* (accessed 11 May 2021)

TVC News (2020) ***'Kano Installs 24/7 CCTV Surveillance Cameras to Curb Crime'***, (accessed June 30)

Umoren, B. (2019) **'NITDA commences investigation on alleged breach of NDPR'**, *Today.ng* (accessed 26 May 2021)

United Nations General Assembly (2014) ***'The right to privacy in the digital age'*** (accessed 26 May 2021)

United Nations General Assembly (2016) ***'Oral Revisions of June 30'*** (accessed 26 May 2021)

Surveillance Law in Africa: a review of six countries

Senegal country report

Ridwan Oloyede

Introduction

Different countries deploy surveillance and interception of communications to combat crimes and ensure national or economic security (Chris 2005). The emergence of serious crimes such as terrorism has increased governments' appetite to conduct communications surveillance. The United Nations (UN) Human Rights Council defines communications surveillance as, 'the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks' (UNHRC 2013). Nonetheless, government surveillance must meet the minimum human rights standards and individuals must be protected against arbitrary interference with their right to privacy (Privacy International 2018a). Unfortunately, failure to adhere to these human rights norms and principles could erode the rights to privacy, expression and assembly (Media and Democracy 2016).

Senegal, a former French colony, has enjoyed an uninterrupted constitutional democracy since independence in 1960, compared to neighbouring countries (Freedom House 2021). The Constitution of Senegal guarantees the right to privacy of communication and prohibits surveillance. However, violations of these rights by the government have been reported (Amnesty International 2020). Senegal has adopted a series of international human rights instruments that reinforce these guarantees (Claiming Human Rights 2011). According to the explanatory statement of Intelligence Services Law, 'intelligence must play a vanguard role in the national security system'. Nonetheless, there have been documented instances of state use of surveillance capability.

A report by non-profit association OSIRIS cited instances of citizens' conversations on telephone lines being monitored (Osiris 2021). In 2010, the United Sates (US) Department of State reported that illegal telephone monitoring by security services was common practice in Senegal. However, the threat of terrorism and availability of digital technologies has provided new impetus to monitor communications (US Department of State 2011). The Government of Senegal has used insecurity around the Sahel region as a reason to introduce internal security legislation (Counter Extremism Project 2020). In addition, a military expedition against the separatist movement in the country's Casamance region has added to the mix of violence confronting the country (Africanews 2021). These perceived threats led the government to amend the Penal Code and Code of Criminal Procedure, creating new terrorism-related offences, increasing the powers of investigating authorities (Amnesty International 2016), legitimising interception of communications and imposing stiffer penalties

for terror-related activities and unlawful interception (Lequotidien – Journal d'information Générale 2017). There are plans to amend both laws further to address terrorism (BBC News Afrique 2021).

In 2016, Senegalese authorities arrested 11 people linked to Nigerian-based terror group Boko Haram, including one individual, Momodou Ndiaye, who was reported to have been tracked through his activities on Facebook (Reuters 2017). 'In 2016, Senegalese authorities also arrested Moustapha Diatta, who ran a Facebook page called 'Proselytise Senegal'. Diatta reportedly helped Senegalese individuals – including three of his children – travel to Libya to fight for ISIS'[1] (Institute for Global Change 2017).

Beyond security threats, other factors are driving wider adoption of surveillance in Senegal. The European Union (EU) is funding a national biometric identity programme worth €28 million to control immigration (Privacy International 2018b). The grant is part of the EU's Emergency Trust Fund for Africa, which was launched in 2015 to stop 'irregular' migration, 'enforcing the rule of law through capacity building supporting security and development and law enforcement, including border management migration-related aspects' (Privacy International 2020). According to telecommunications company Orange's Transparency Report on Freedom of Expression and Privacy Protection in 2016, the Senegalese government made the second-highest number of customer data interception surveillance requests in Africa (Orange 2017).

Senegal has mandatory requirements to register mobile device SIM cards (Privacy International 2019a). The mandatory requirement to register SIM cards erodes anonymity and negatively impacts the right to privacy of communications. Senegal has also been accused of purchasing FinFisher surveillance malware capable of monitoring communications (Privacy International 2015). Some laws allow the government to carry out surveillance, enable monitoring capability and increase investigatory powers.

This report looks at these laws and evaluates them against the UN Draft Legal Instrument (2018) on state surveillance, which allows targeted surveillance. The report sets out how the laws apply in practice and concludes with specific recommendations for different stakeholders. The remainder of this report is organised as answers to 12 questions about surveillance law in Senegal.

1 Islamic State of Iraq and Al-Sham – a global terrorist group responsible for attacks in many parts of the world.

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

Like many other countries, the Senegalese government's primary driver for surveillance is national security, according to the explanatory statement of the Law on Intelligence Services. Increasing terrorism activities in neighbouring countries and the Sahel region, and insurrection in the country's Casamance region, have also been drivers. As a result, the government enacted an anti-terror law that empowers law enforcement agencies to intercept communications. However, the state has reportedly used surveillance outside the legitimate purpose advanced by the government. For example, the government has reported purchasing surveillance tools to monitor citizens (The Africa Report 2020). Similarly, EU funding to control immigration has given the government a more comprehensive capability to monitor people (Privacy International 2019c). Health and disease surveillance was also deployed to combat the coronavirus (Covid-19) pandemic when the government declared a state of emergency and conducted contact tracing (DHIS 2 2021).

2. Which international conventions protecting privacy has Senegal adopted?

The country has ratified or signed several international instruments, some of which are listed below.

a. **African Charter on the Rights and Welfare of the Child (1999)**

Article 10 of the charter guarantees African children's right to privacy. Accordingly, a Senegalese child enjoys the protection of the law over their communications and correspondence, which cannot be unduly interfered with.

b. **Universal Declaration of Human Rights (1948)**

Article 12 provides that no one should be subjected to arbitrary interference in their privacy and correspondence. Thus, all Senegalese enjoy legal protection against such arbitrary interference.

c. **African Union Convention on Cybersecurity and Protection of Personal Data (Malabo Convention) (2014)**

The convention establishes a baseline for legislation to protect personal data in Africa. Senegal is a signatory and although it is one of the African countries that ratified the Malabo Convention early, the convention has yet to take effect because it requires ratification by 15 countries; it has only been ratified by ten (African Union 2021).

d. **Economic Community of West African States Supplementary Act on Personal Data Protection (2010)**

The act creates a legal framework for the protection of personal data in the subregion. Senegal is a signatory to the act.

e. **International Covenant on Civil and Political Rights (1966)**

Article 17 of the covenant protects Senegalese citizens from arbitrary and unlawful interference with their communications and correspondence.

f. **Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention no. 108) (1981)**

The convention provides a framework for the protection of personal data. It is the only binding data protection instrument globally and Senegal has acceded to the instrument.

g. **Convention on Cybercrime of the Council of Europe (Budapest Convention) (2001)**

The convention is the only binding international instrument on cybercrime. It prescribed the framework for countries to legislate on cybercrime. Article 21 of the convention provides for the interception of content data. Therefore, countries should adopt the legislation necessary for severe offences to empower their competent authorities to intercept content data. The power to intercept is subject to article 15 of the convention, which prescribes that countries should adopt safeguards.

Other international commitments

Senegal is also committed to the African Charter on Human and Peoples' Rights, which established the African Commission on Human and Peoples' Rights (ACHPR), a quasi-judicial body responsible for the protection and promotion of human and peoples' rights. The ACHPR reviews the state's reports concerning its human rights situation and decides on complaints of alleged violations. Additionally, Senegal has accepted the jurisdiction of the African Court on Human and Peoples' Rights to hear complaints presented by the commission (International Justice Resource Center 2017).

These international commitments set out established principles that guide the Senegalese government. Article 79 of the Constitution of Senegal stipulates that international law takes precedence over domestic law. Consequently, international human rights instruments are part of the domestic law of Senegal and take precedence over any discriminatory state law (Privacy International 2013). Consequently, there is a solid legal framework that protects the privacy of communications and correspondence from arbitrary and unlawful interference by the government or any other entity.

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

a. **Constitution of Senegal 2001**

Article 13 of the Constitution of Senegal establishes the right of citizens to privacy, stating that 'the secrecy of correspondence and electronic communications is inviolable. A restriction on this inviolability can only be ordered following the law.' This is in accord with the recommendation of the International Principles on the Application of Human Rights to Communications Surveillance that any surveillance that interferes with the right to privacy must be expressly allowed and defined in law (EFF 2014).

b. **Intelligence Services Law 2016**

Article 10 defines a limited number of 'legitimate aims' for surveillance, such as the threat of terrorist attack. The law makes it possible for Senegal's special intelligence services to conduct surveillance if there are no other ways to address the threat. In such cases, Article 10 makes it legal to resort to technical, intrusive surveillance or location procedures to gather valuable information to neutralise the perceived threat. Similarly, Article 8 provides that investigating entities may, with authorisation from and under the control of a competent public prosecutor, resort to the means of investigation under Article 10. The evidence duly collected by these means is admissible in court and is left to the discretion of the competent criminal court. Article 9 stipulates that in executing their mission, intelligence services must have recourse to the legality of the means employed and proportionality to the seriousness of the threat. This is consistent with the international principle of proportionality. Article 14 provides that an administrative body will be responsible for controlling the activities of the intelligence services. The public prosecutor is designated as the administrative oversight authority; there is no judicial intervention or oversight as prescribed under the International Principles.

c. **Protection of Personal Data Law 2008, and Decree Concerning Law Enforcement 2008**

Article 1 sets out the objective of the law, which is to protect the right to privacy. Article 35 prohibits the misuse of personal data. The law also creates specific obligations on public and private authorities to implement data protection principles. Significantly, data-processing activity must be lawful. The law established the Data Protection

Commission (CDP), which acts as the data protection authority responsible for enforcing the law. The law puts in place safeguards to preserve data protection rights, but allows derogations in cases of public interest, national security or investigation of crime, as contained in Article 40 of the Decree.

d. Code of Criminal Procedure Law 2016

Combatting terrorism was set out as the legitimate aim of the legislation. Article 90-2 empowers the investigating authority to search computer systems if it is essential for investigating a crime. However, the search is subject to international commitments in force in Senegal. Articles 90-4 and 90-17 empower the investigating authority to decrypt encrypted data for investigation. According to Amnesty International,

> these articles are loosely worded and appear to extend the investigative judge's powers of investigation beyond specific data concerning a targeted individual allegedly linked to the criminal activity in question. These powers seem to extend to the very functioning of the computer system, which compromises all the data relating to it.
> (Amnesty International 2016)

Article 90-16 empowers the investigating authority to conduct interception of communications under a judicial authorisation. The order must specify the communications to be intercepted, the offence motivating the interception and the duration of the interception The planned investigative measures must be proportionate to the seriousness of the offence. However, the exercise of this power is not subject to judicial appeal.

Article 90-11 provides that if the necessities of the search for evidence so require, the investigating authority in the execution of a judicial directive may use appropriate technical means to collect or record in real time data relating to the content of specific communications transmitted using a computer system or oblige a service provider, within the framework of its technical capabilities, to collect or record computer data, or assist the competent authorities in collecting or recording the data. Article 90-10 permits the investigating judge for the purpose of investigation to direct the installation of software to intercept, which is contrary to the international principle of integrity of communications system.

e. **Code of Electronic Communications 2018**

Article 27 allows the government to oversee traffic management, surveillance and potential blocking of services. The code also expanded government oversight on intermediaries, which could lead to monitoring and violation of privacy rights. Article 36 of the code imposes the obligation on service providers to guarantee the privacy and data protection of users.

f. **Law on Cryptography 2008**

Article 12 provides that private individuals have the right to use encryption. However, its use is subject to the standard set by the National Cryptology Commission (NCC) (article 16). In such an instance, encryption is only permitted if the encryption key length is less than or equal to 128 bits. The NCC is responsible for setting the maximum length of encryption keys. The use of encryption with a longer key requires authorisation from the NCC (Global Partners Digital 2018). The purpose of encryption is to ensure the confidentiality of communications, which is guaranteed under the constitution. Individuals have an inviolable right to the privacy of their communications and private correspondence. However, this law appears to curtail the exercise of this law by imposing a limitation on the quality of encryption that individuals can use. In addition, the Code of Criminal Procedure empowers the investigative judge to decrypt encryption. Thus, while on the one hand, it appears to uphold the international principle of security of communications, it also creates a loophole to violate that right.

g. **Telecommunications Code 2011**

Article 7 mandates service providers to protect consumers' privacy and personal data, and it can only be waived by a provision of a law. Article 12 provides that,

> [a] judge or judicial police officer, for the needs of the prosecution or an investigation, or the enforcement of a judicial ruling, may require that telecommunications operators and service providers or telecommunications networks make available helpful information stored in the computer systems they administer. Telecommunications operators and service providers of telecommunications networks are required to submit the required information to the authorities.

The provision empowers the investigating authority to request that telecommunications companies make information on computer systems available to the investigating authority to investigate crime. In addition, the provision allows the authority to request the companies to grant access to communications. Nonetheless, the provision does not provide

other safeguards, such as notifying individuals that they are under surveillance, or clarify whether the powers apply to minor crimes or only the most severe crimes.

h. Cybercrime Law 2008

Article 667-38 empowers the investigating authority to use appropriate technical means to record content data or specific communications in real time. Service providers are obliged to support investigating authorities in intercepting communications data. Article 677-36 allows the investigating authority to intercept communications data stored in Senegal that are important to an investigation. Disclosure under the law is subject to secrecy. The exercise of investigative power under these provisions is subject to the judicial supervision of an investigating judge.

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

Some African countries have been reported to engage in arbitrary mass surveillance (CitizenLab 2020). In addition, there are fears that several governments are procuring surveillance tools to monitor dissidents, political opponents, human rights defenders and journalists. Algeria, Botswana, Côte d'Ivoire, Egypt, Ghana, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia and Zimbabwe were reported to have procured and deployed surveillance tools (Jili 2020). In July 2021, after a forensic investigation, the Guardian and other media outlets reported the use by some African countries such as Rwanda, Togo, and Morocco of Israeli company NSO Group's malware, Pegasus, which allows security agencies to listen to phone calls, intercept messages, and also to track individuals (Damien 2021). The malware has been reportedly used to spy on dissidents, opposition, journalists, and foreign leaders (Lynsey 2021). Although Rwandan and Moroccan governments have denied the claim (Kirchgaessner 2021, Shaquile 2021), in 2019, dissident and human rights activists from Rwanda and Morocco were privately warned by communication giant WhatsApp that they were victims of cyber-attacks designed to infiltrate their phones by an NSO Group malware (Kirchgaessner *et al.* 2019).

The pervasive practices appear to go unchallenged due to vague laws that are subject to abuse, codification of state power to conduct mass monitoring, the absence of independent oversight bodies, and weak legal frameworks and institutions. For example, in Uganda facial recognition has been deployed to monitor protesters (Quartz Africa 2020).

Nonetheless, there are examples of progressive practices on the continent. In South Africa, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) is the primary law on surveillance. The RICA creates an oversight body and puts in place several safeguards contained under the International Principles. However, the law also omits some safeguards. The laws in Senegal and South Africa are silent on the role of transparency from investigating authorities (Privacy International 2019b). In addition, the RICA prohibits the disclosure of demands for communications data under the law, further hampering transparency. Furthermore, there is no statutory requirement to publish a public annual report. Finally, the laws in both countries omit the obligation to notify individuals that they are or have been under surveillance, denying

the targeted individuals the opportunity to challenge an interception or seek redress.

The laws in Senegal and South Africa have the requirement to specify the category of offence before requesting a judicial authorisation. There also appears to be a normative condition to establish a legitimate aim before conducting surveillance. However, some existing practice falls short of the requirement under the International Principles. For example, in 2021 South Africa's Constitutional Court delivered a landmark judgment outlawing mass surveillance in the country. In *Amabhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services (CCT 278/19),* the court held that the government should no longer conduct mass surveillance of citizens. The court also declared certain parts of the RICA unconstitutional (BusinessTech 2021). Notably, the court stated that the RICA fails to provide sufficient safeguards to preserve the right to privacy, the law did not provide adequate protection or relief for persons subjected to surveillance, and the law did not make provision for individuals subjected to surveillance to be notified after the fact, among other issues.

Nonetheless, South Africa has a specific surveillance law as suggested by the UN Draft Legal Instrument. This could be considered preferable to having contradictory legitimate aims and safeguards specified in different pieces of legislation. South Africa has a more explicit definition of tests for a judge to assess before issuing authorisation, which is not evident in the Senegalese framework. South Africa has an 'independent oversight board' as conceptualised under the International Principles. The law in South Africa also has the advantage of being challenged and tested in court by civil society in ways that have identified flaws, clarified provisions and provided enhanced privacy protections.

5. How does Senegalese surveillance law compare with the UN Draft Legal Instrument and international Principles

The existing legal framework in Senegal contains some of the elements suggested in the UN Draft Legal Instrument and the International Principles. For example, the Penal Code Law provides a safeguard against illegitimate access or interception by private entities: article 431-12 of the law carries a prison term of 1–5 years for unlawful interception of communications, which is consistent with the international principle of safeguards against illegitimate access. However, many elements are absent. These omissions relate mainly to the lack of safeguards and imprecise definitions, leaving the law open to abuse in the hands of a repressive government or officials.

Conversely, under the Code of Criminal Procedure, investigative measures must be proportionate to the seriousness of the offence and are subject to the necessity of investigation under the judicial supervision of an investigating judge. However, the exercise of power to intercept communications under article 90-16 of the Code of Criminal Procedure is not subject to appeal, which violates one of the principles of the UN Draft Legal Instrument: that, as soon as is practical, the subject of surveillance should be notified that they have been under surveillance and have the legal right to information and ability to appeal. The UN Draft Legal Instrument prescribes that the individual should be informed ahead of the surveillance activity to be able to contest it (except in specified urgent circumstances). The investigating authority is also expected to notify the CDP when there has been a data breach. Unfortunately, the Protection of Personal Data Law does not include the obligation to notify the CDP when there has been a data breach.

Requirements such as conducting a human rights impact assessment before deploying surveillance tools are not contained in any legislation. The law also enables the weakening of encryption and the cryptography law prescribes the standard of encryption. Furthermore, encryption is tied to freedom of expression and privacy; restricting the standard of encryption restricts these rights. According to the United Nations Educational, Social and Cultural Organisation (UNESCO), 'strong encryption is needed to protect privacy and freedom of expression in the digital age' (UNESCO 2016). Lastly, there is no requirement for transparency. For example, investigating authorities

are not required to publish a public annual report. As a result, much of the surveillance capability of the state is shrouded in secrecy.

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

Phrases like 'national security,' 'reasonable suspicion' or 'interception' are hardly defined or centred on respect for human rights. The Penal Code sets out prevention of terrorism as its legitimate aim. The failure to define these words leaves room for potentially arbitrary abuse. However, a semblance of how the terms should work is found in some laws. For example, the Code of Criminal Procedure sets out prevention of terrorism as a legitimate aim and provides context for what can be considered a severe crime under Article 90-16. The provision allows interception by investigating authorities:

> in felony matters, for a renewable period of four months; in misdemeanor matters when the minimum penalty is greater than or equal to five years' imprisonment, for a renewable period of four months; in a bid to investigate into the cause of death or disappearance, for a renewable period of two months; in the context of the search for a fugitive, for a period of two months.

Similarly, under the Code of Criminal Procedure, the interception decision must specify the offence, which has to be proportionate to the threat, and the duration of surveillance must be indicated.

The data protection law and the constitution impose the obligation to ensure the preservation of individuals' privacy and cannot be violated without a lawful basis. The constitutional guarantee is inviolable and serves as the basis to protect individuals against unwarranted surveillance. However, the constitutional provision is subject to derogations prescribed under a law. The Law on Intelligence Services allows for intrusive surveillance to neutralise a threat if it is the only means. Similarly, the Cybercrime Law allows surveillance for investigation of crimes. These legitimate surveillance aims are insufficiently defined. A constitutional provision cannot be considered inviolable if an official can waive it in the case of a petty crime or be justified concerning subjective issues of morality that are not defined in law.

Investigating authorities have an essential role in surveillance; they act based on judicial directives and supervision. However, under the Code of Criminal Procedure, decisions on interception are not subject to an appellate process. Therefore, notification of individuals ahead of surveillance is an effective tool to combat overreach but it is not required under any of the laws examined.

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

Under the International Principles, there are legal safeguards such as competent judicial authority, public oversight, transparency, and protection against illegitimate access. The role of independent oversight body is absent. There is no obligation or central oversight body concerning public disclosures of statistics on requests for and collection of communication data. Under the Law on Intelligence Services, the investigating authority determines what is proportionate to a threat and the decision is not subjected to a judicial decision-making process. Similarly, investigating authorities are not mandated to make public the details of legal requests or interceptions made. Safeguards such as conducting human rights impact assessments before deploying surveillance tools are not conducted. As a result, it is hard to know which law the government relies on to conduct surveillance. According to a report by the Association for Communications Progress (APC), 'the Government of Senegal never informs the population about how it concretely uses this legal framework of surveillance, a total opacity is maintained' (APC 2016).

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

The constitution and the law on the protection of personal data seek to protect individuals' privacy. Similarly, other laws reiterate the preservation of the right to privacy. The data protection law, for example, imposes many obligations on public and private authorities. This comprehensive data protection law covers the collection, processing, transmission, storage and use of personal data by legal entities under public or private law. In addition, Article 35 prohibits the misuse of data; and article 34 proscribes the collection of personal data without the knowledge of the data subject. The law also creates the obligation for public authorities to ensure data security, consistent with the international principle of the integrity of communications and systems.

Protection of Personal Data Law and the Decree Concerning Law Enforcement create derogations to the application of data protection law. Article 73 of the decree empowers a court to order necessary security measures in a period of emergency. Similarly, article 40 of the decree provides that the law will not apply to 'public security, defence, investigation and prosecution of criminal offences or the security of the State.' Similarly, the Protection of Personal Data Law empowers the CDP to impose administrative and penal sanctions for violation of the law. The Law on Cybercrimes provides a safeguard against illegitimate access or interception by private entities. Article 431-12 of the law carries a prison term of 1–5 years for unlawful interception of communications.

The state may carry out surveillance for legitimate aims such as preventing terrorism and other serious crimes (defined by the law). However, mass surveillance and monitoring of communications in violation of existing legal mechanisms and international human rights norms are considered intrusive, violating privacy and protection of personal data. Nevertheless, the Senegalese government is not transparent as it never informs the public how it uses the existing legal framework of surveillance in practice (GIS Watch 2014). This opacity is further reinforced by the lack of an obligation to publish public transparency reports on legal requests.

Despite a lack of resources, the CDP has been relatively efficient and transparent about its activities. It publishes a quarterly report highlighting its activities, which includes the number of public complaints on violation of

data protection rights received and resolved. However, the law was enacted in 2008 and has yet to be amended. It does not entirely address emerging modern concerns such as the requirement to conduct a data protection impact assessment, appointment of a data protection officer and data protection by design (Robertson 2020). Aside from these concerns, there are not sufficient safeguards around surveillance and the abuse and violations of rights that could accompany it. For example, the mandatory requirement to register SIM cards is not accompanied by sufficient data protection measures. According to a report by Privacy International, a non-profit watchdog (2019a):

> Mandatory SIM card registration laws require that people provide personal information, including a valid ID or even their biometrics before they can purchase or activate a prepaid SIM card for their mobile device. Such laws can allow the State to identify the owner of a SIM card and infer who is likely to be making a call, sending a message, in a particular location at any particular time.

There is no reference to users' right to access their data or to rectify errors in their data. Operators are not obliged to inform users of how their data are used or how they are processed. No information is given to users on the procedures for deleting their data when they change operators. The lack of sufficient safeguards could enable the government to monitor communications arbitrarily under the guise of maintaining security.

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

Senegal's biggest domestic threat is the security situation in the Sahel region, which has required it to strengthen counterterrorism measures. Similarly, the country is confronting an insurgency in the Cassmance region (Freedom House 2021). The legitimate aim advanced under the Penal Code and Intelligence Law is prevention of terrorism. The capacity to conduct surveillance is found under different laws, but it is not easy to ascertain which law is being relied upon. The Code of Criminal Procedure makes it a requirement to specify the purpose of interception and it must be proportionate to the threat.

In appraising necessity, the UN Draft Legal Instrument has established that surveillance measures being deployed must be necessary and they can only be carried out when there are no other, less intrusive measures that could secure the same legitimate aim (such as foiling a terrorist attack). Article 10 of the Law on Intelligent Services provides that intrusive surveillance can only be conducted if there is no less intrusive way to carry out the investigation. The weakening of encryption infringes on freedom of expression and the right to privacy.

Surveillance under the Code of Criminal Procedure requires prior judicial authorisation, and measures adopted must be proportionate to the severity of the crime, which is consistent with the international principle of proportionality.

The EU-funded digital identity programme has raised many privacy concerns. Biometric information is a unique identifier; when it is combined with other data such as financial transactions, mobile location, or facial and vehicle recognition technologies, the government has the opportunity to build an extensive surveillance capability. A repressive government could abuse the capability to weaken encryption to conduct surveillance on activists and political opponents. Crackdowns on the opposition have increased in Senegal in the past few years and formed part of the most recent election cycle in 2019 (Amnesty International 2021).

10. How has surveillance law played out in court in Senegal?

Unlike other African countries, Senegal has enjoyed a democratic transition without military interference. The courts have been mainly independent and adequately run. However, there has been no documented case challenging the state over conducting surveillance. This may partly be the result of the secrecy over government surveillance, which is reinforced by the absence of the requirement to publish a transparency report. According to a report, Senegalese authority used intelligence to monitor the movement and phone conversations of Muktar Diokhane, a Senegalese linked to Boko Haram. The report also stated that Senegal tracks open-source information and social media, and collaborates with 'French and Nigerien authorities on tracking and monitoring the phone calls of suspects' (Zenn 2018). Diokhane was sentenced to twenty years' imprisonment. The evidence presented before the court was gathered through intelligence. Although surveillance of Diokhane was not directly challenged, the case demonstrated an instance where evidence gathered through surveillance was used for prevention of crime.

The Law on Protection of Personal Data empowers the CDP to impose administrative and financial sanctions for violating the law. The Penal Code creates several offences for abuse and misuse of personal data. The code imposes varying prison terms and financial sanctions. Individuals who perceive their rights have been abused can approach the court for relief.

A report by non-profit association OSIRIS cited instances of citizens' telephone conversations being monitored (Osiris 2021). Similarly, a telecommunications company was also found to be monitoring employees' communications (EnQuete+ 2019). However, the provisions of the Code of Criminal Procedure make it impossible to appeal against the decision to intercept communications, which could encourage the invasion of Senegalese citizens' privacy (Cio Mag 2019).

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

Senegal has a long-running history of uninterrupted constitutional democracy. Many provisions of laws enabling surveillance are consistent with the UN Draft Legal Instrument. For example, the Code of Criminal Procedure has as its defined legitimate aim the prevention of terrorism. It adds other safeguards such as establishing the severity of the crime, the duration of surveillance and proportionality of the seriousness of the threat before carrying out surveillance, consistent with the international principles of legitimate aim, proportionality and reasonable grounds. It also safeguards against unlawful interception by penalising unlawful interception with imprisonment term, which is consistent with the international principle of safeguards against illegitimate access.

Another key point is the existence of the data protection law and establishment of the CDP. In addition, though, there are plans to amend the data protection law. The role of judicial supervision in the process also represents a trust-building process.

Some of the gaps the report identified are the absence of transparency, with the absence of a requirement to publish a report on legal requests and lawful interception. The failure to designate an independent agency to hold law enforcement agencies to account under the Intelligence Services Law is another gap. In addition, the legal framework for surveillance is not clear on the requirement to notify individuals they are or have been under surveillance. Finally, additional safeguards, such as conducting a human rights impact assessment before deploying surveillance tools, are not contained in any law.

12. What recommendations arise from this analysis for legislation, policy, practice or further research?

For the government

- The government should promote citizens' trust by being open and transparent and ensuring that surveillance measures are proportionate and within the ambit of the law. The government should publish an annual transparency report on the volume of requests and authorisations and instances of surveillance should be available publicly or accessible to the members of the public.
- The government should conduct a human rights impact assessment before deploying surveillance tools.

For policymakers and legislators

- The laws on surveillance should be enacted into a single law as recommended in the UN Draft Legal Instrument.
- The law should mandate the investigating authorities to notify individuals who are subject or have been subjected to surveillance of such a decision and give them chance to contest it or appeal against it. Finally, investigating authorities should be mandated to publish the details of interception requests.
- There should be strict rules concerning the purchase and deployment of invasive surveillance technologies. A human rights impact assessment should be made a mandatory requirement before deploying surveillance tools.
- Service providers should be mandated to publish a transparency report periodically.
- The law on personal data should be amended to address the requirement to conduct a data protection impact assessment before deploying surveillance tools for surveillance.
- The budget of the CDP should be increased and it should be more autonomous from government institutions.
- Terms such as 'national security' and 'interception' should be defined to be anchored in respect and protection of human rights.
- The Code of Criminal Procedure should be amended to ensure respect for the rights to privacy and freedom of opinion and expression.

The amendment should require the lifting of encryption only for the investigation of the most severe crimes.

- The restriction on using encryption software should be removed. The use of encryption technology should be accessible to all individuals.

For civil society and activists

- Activists and civil society organisations should actively campaign for amendments to the law through engaging with policymakers.
- Strategic litigation should be used to clarify the law, narrow down targets of surveillance, and protect and safeguard citizens' rights. Also, civil society organisations should challenge intelligence services over violations of the law or existing human rights instruments that Senegal is party to.
- Activists and civil society organisations should work to raise public awareness about privacy rights, surveillance and available protections.

For researchers

- It is recommended that more research is carried out to reveal new evidence relating to the various tools, methods and tactics employed by the government to conduct surveillance.

For journalists

- Journalists and other media personnel should do a lot more to raise public awareness through reporting on surveillance practices and their effects. More research needs to be done to understand the categories and volume of cases in which surveillance data are used as evidence.

References

Africanews (2021) ***Senegal Says Troops Overrun Rebel Camps in Casamance Region*** (accessed 5 July 2021)

Amnesty International (2021) ***Call for justice for the violent crackdown on #FreeSenegal protests*** (accessed 10 July 2021)

Amnesty International (2016) ***Analyse Des Lois Modifiant Le Code Penal Et Le Code De Procedure Penale*** (accessed 28 July 2021)

Amnesty International (2020) ***Amnesty International Report 2020/21: The State of the World's Human Rights*** (accessed 9 July 2021)

Association for Communications Progress (APC) (2016) ***Surveillance Numérique Pour Combattre Le COVID-19 : Opacité Gouvernementale Au Sénégal*** (accessed 5 July 2021)

BBC News Afrique (2021)***Loi Contre Le Terrorisme Au Sénégal: Pourquoi C'est Si Controversé?*** (accessed 5 July 2021)

BusinessTech (2021) ***South Africa's RICA Law Is Unconstitutional: Court Ruling*** (accessed 28 July 2021)

Chris, B. (2005) ***Surveillance and the Interception of Communications***, Transnational Institute (accessed 20 July 2021)

Cio Mag (2019) ***Sénégal: Des Risques d'Atteinte à La Vie Privée, Après l'Adoption de La Stratégie Nationale de Cybersécurité*** (accessed 5 July 2021)

CitizenLab (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*** (accessed 1 July 2021)

Claiming Human Rights (2011) ***Claiming Human Rights – in Senegal*** (accessed 9 July 2021)

Counter Extremism Project (2020) ***Senegal: Extremism and Terrorism*** (accessed 10 July 2021)

Damien, G. (2021) ***Morocco, Rwanda, Togo...How Involved Is Africa in 'Pegasus Gate'?*** The Africa Report (accessed 28 July 2021)

DHIS 2 (2021) ***Harmonisation Dans La Collecte de Données Pour Une Meilleure Riposte Contre La COVID-19*** (accessed 11 July 2021)

Electronic Frontier Foundation (EFF) (2013) ***International Principles on the Application of Human Rights to Communications Surveillance*** (accessed 5 July 2021)

EnQuete+ (2019) ***Les Enregistrements Téléphoniques Comme Moyens De Preuves : ''Illégaux'' et ''Irrecevables'', Selon Des Juristes'*** (accessed 9 July 2021)

Freedom House (2021) ***Senegal: Freedom in the World 2021*** (accessed 10 July 2021)

GIS Watch (2014) ***Communications Surveillance in the Digital Age*** (accessed 5 July 2021)

Global Partners Digital (2018) ***World Map of Encryption Laws and Policies*** (accessed 10 July 2021)

International Justice Resource Center (2017) ***Senegal Regional: African System*** (accessed 10 July 2021)

Jili, B. (2020) ***Surveillance Tech in Africa Stirs Security Concerns***, Africa Center for Security Studies (accessed 1 July 2021)

Kirchgaessner, S.; Hopkins, N. and Holmes, O. (2021) '**Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance'**, *The Guardian*, 19 July (accessed 29 July 2021)

Kirchgaessner, S; Hopkins, N. and Holmes, O. (2019) **'WhatsApp 'Hack' Is Serious Rights Violation, Say Alleged Victims'**, *The Guardian*, 1 November (accessed 29 July 2021)

Lequotidien – Journal d'information Générale (2017) ***REFORME – Modification Du Code Pénal et Du Code de Procédure Pénale : Amnesty International Met En Lumière Les 'Dispositions Liberticides'*** (accessed 10 July 2021)

Lynsey C (2021) ***Pegasus Lands in Africa*** (accessed 28 July 2021)

Media and Democracy (2016) ***Communications Surveillance and Privacy in South Africa*** (accessed 20 July 2021)

Orange (2017) ***Orange Transparency Report on Freedom of Expression and Privacy Protection*** (accessed 5 July 2021)

Osiris (2021) ***Écoutes et Espionnage Téléphonique au Sénégal/Une Pratique Sous Le Feu Des Radars : Outils De Dissuasion Ou Élément Redoutable Contre Les Infractions?*** (accessed 9 July 2021)

Privacy International (2020) ***Here is How a Well-Connected Security Company Is Quietly Building Mass Biometric Databases in West Africa with EU Aid Funds*** (accessed 9 July 2021)

Privacy International (2019a) ***Africa: SIM Card Registration Only Increases Monitoring and Exclusion*** (accessed 9 July 2021)

Privacy International (2019b) ***State of Privacy South Africa*** (accessed 10 July 2021)

Privacy International (2019c) ***The EU Funds Surveillance around the World: Here's What Must Be Done about It*** (accessed 11 July 2021)

Privacy International (2018a) ***Communications Surveillance*** (accessed 20 July 2021)

Privacy International (2018b) ***The EU's next Budget Threatens Privacy around the World for Decades to Come*** (accessed 10 July 2021)

Privacy International (2015) ***Ugandan Government Deployed FinFisher Spyware to 'Crush' Opposition, Track Elected Officials and Media in Secret Operation during Post-Election Protests, Documents Reveal*** (accessed 10 July 2021)

Privacy International (2013) ***The Right to Privacy in Senegal Stakeholder Report Universal Periodic Review 17th Session – Senegal*** (accessed 11 July 2021)

Quartz Africa (2020) ***Uganda Uses China's Huawei Facial Recognition to Snare Protesters*** (accessed 1 July 2021)

Reuters (2017) ***Senegal Arrests Three Suspected Foreign Jihadists*** (accessed 9 July 2021)

Robertson, T. (2020) ***Senegal to Review Data Protection Law, Collaboration on International ICT Policy for East and Southern Africa***, CIPESA (accessed 10 July 2021)

Shaquile, G. (2021) **'Pegasus Project: Morocco's Public Prosecutor Orders Probe into 'False Allegations''**, *Morocco World News*, 21 July (accessed 29 July 2021)

The Africa Report (2020) ***Inside Africa's Increasingly Lucrative Surveillance Market*** (accessed 9 July 2021)

Tony Blair Institute for Global Change (2017) ***Senegal, ISIS, and Al-Qaeda: A Terrorism Trifecta*** (accessed 10 July 2021)

US Department of State (2011) ***2010 Country Reports on Human Rights Practices*** (accessed 9 July 2021)

United Nations Educational, Social and Cultural Organisation (UNESCO) (2021) ***'Human Rights and Encryption'*** (accessed 10 July 2021)

United Nations Human Rights Council (UNHRC) (2013) ***Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*** (accessed 20 July 2021)

Zenn, J. (2018) ***'Boko Haram's Senegalese Foreign Fighters: Cases, Trends and Implications'***, The Jamestown Foundation (accessed 28 July 2021)

Surveillance Law in Africa: a review of six countries

South Africa country report

Grace Mutung'u

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)

Surveillance Law in Africa: a review of six countries

Sudan country report

Mohamed Farahat

Introduction

Many human rights can be affected by surveillance, including the right to freedom of expression, the right to assembly, the right to information and communication, and the right to privacy.
According to one definition, '"Communications surveillance" in the modern environment encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future' (Electronic Frontier Foundation (EFF) 2013). According to the United Nations (UN) Draft Legal Instrument on Government-led Surveillance and Privacy (UN 2018),[1] surveillance is defined as 'any monitoring, collecting, observing or listening by a state or on its behalf or at its order to persons, their movements, their conversations or their other activities or communications including metadata and/or the recording of the monitoring, observation and listening activities'. Both sources refer to a broad definition of surveillance that includes all practices that constitute surveillance, whether direct or indirect. This report will therefore address all related legislation that enables or limits surveillance practices, either directly or indirectly.

The right to privacy in Sudan is protected in three ways: by the 2019 Sudanese Constitution; through international conventions that Sudan is a party to; and in Sudanese laws. But Sudanese laws also enable surveillance. While surveillance always violates the right to privacy, it is argued that narrowly targeted surveillance in strictly limited cases is legitimate to prevent greater violations such as terrorist attacks. Carefully crafted surveillance legislation and safeguards are needed to balance the tension between the right to privacy and the need for surveillance. This report will show that excessive surveillance and privacy violations occur in Sudan; it will also identify opportunities to improve privacy protections and the legal practice of narrowly targeted surveillance.

Before 2011, Sudan witnessed offline and online surveillance practices by the government, which targeted activists, lawyers and journalists (Amnesty International 2010). According to the OpenNet Initiative (2009: 4), 'the government of Sudan monitors Internet communications, and the National Intelligence and Security Service reads e-mail messages between private

1 This draft text for a Legal Instrument (LI) on Government-led Surveillance and Privacy is the result of meetings and exchanges between the MAPPING project and several categories of stakeholders shaping the development and use of digital technologies. These include leading global technology companies, experts with experience of working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping the internet and the transition to the Digital Age.

citizens. Media reports reveal that Sudan's police have a special unit that monitors internet cafés to stop them from providing access to sexual content'. In 2007, the National Telecommunication Corporation (NTC) 'set up a special unit to censor and filter internet content before it reaches users inside Sudan' (Abubkr 2014: 228). In 2011, under Al-Bashir's regime, the National Intelligence Security Services (NISS) established a special unit called the 'Cyber-Jihadists' to exercise online surveillance practices, conduct 'online defence operations' and 'act as a special internet and social media surveillance unit to spy on government critics, human rights activists, journalists and opposition parties' (Paradigm Initiative 2019) and censor private accounts such as emails, Twitter and Facebook (Ali 2020). Sudan is one of 21 countries that has used Hacking Team's RCS spyware (Marczak *et al.* 2014).

These state surveillance practices were present during the Sudanese revolution in 2018 as they have been in other North African countries. Sudan has used various legal tools to close civic space and control the online activities of those calling for change. According to the African Freedom of Expression Exchange (AFEX 2019: 8), 'Online expression is susceptible to monitoring, removal of content and self-censorship as individuals, and journalists fear arrests and prosecution under the existing criminal laws including the Law on Combating Cybercrimes of 2018'. In common with other countries, Sudan has seized on the Covid-19 pandemic to increase surveillance practices. Ali (2020: 121) argues that 'The government continues to rely on foreign software to spy on citizens and has taken the Covid-19 pandemic as an opportunity to use technology to increase surveillance and limit people's digital rights'.

This report reviews the Sudanese legal framework regulating surveillance practices, and examines its conformity with international standards, particularly the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2013). It makes this assessment by answering a series of questions that reflect the surveillance practices in the Sudanese context. The report first outlines the contents of existing national legislation and then measures these against relevant international comparators. The report pays particular attention to the parameters within which surveillance is permitted in law and to the legal safeguards detailed in the legislation, before concluding with recommendations that aim to improve the legal framework and surveillance practices in Sudan.

The remainder of this report takes the form of answering 12 questions to enable the reader to make direct comparisons with the other five country reports.

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

According to principle (1) of the International Principles on the Application of Human Rights to Communications Surveillance (legality principle), 'Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.' The OpenNet Initiative (2004: 6) argues that 'Countries usually justify the laws that enable filtering by invoking one of two broad themes: upholding "community standards" and ensuring "national security"'. Sudan uses both justifications. Reviewing Sudanese domestic legislation illustrates the use of community standards and of morals, national security, and indecency as justifications for surveillance. The details of these justifications will be elaborated in Section 3 of this report.

The Sudanese Constitution and the Cybercrimes Law provide the legal basis for the right to privacy in Sudan, but other national security laws provide the basis for breaching this right, as we discuss in detail later in this report.

2. Which international conventions protecting privacy has Sudan adopted?

Sudan is party to most of the international human rights instruments that provide the basis for the universal right to privacy. This includes the Universal Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, the Arab Charter on Human Rights and the Cairo Declaration on Human Rights in Islam. In 2013, Sudan also ratified and became part of the Arab Convention of Anti-Information Technology Crimes (cybercrimes).

Table 1.1 International conventions signed and ratified by Sudan

International Conventions	Signature	Ratification
Universal Declaration of Human Rights	1948	-
International Covenant on Civil and Political Rights	N/A	1986
Convention of the Elimination of All Forms of Discrimination against Women	N/A	N/A
UN Convention on the Rights of the Child	24 Jul 1990	3 Aug 1990
Optional Protocol to Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography	N/A	2004
African (Banjul) Charter on Human and Peoples' Rights	3 Sep 1982	18 Feb 1986

Source: Adapted from University of Minnesota, Human Rights Library (no date) and Human Rights Library.

All the international instruments detailed in Table 1.1 clearly ensure the right to privacy and data protection.

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

Principle (2) of the International Principles states that 'Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'

It is not only the key international conventions that Sudan is party to that prohibit surveillance and protect the right to privacy, the Sudanese Constitution also emphasises the same rights and obligations. However, domestic laws are not aligned with these international and constitutional obligations, as we discuss subsequently.

Sudan's Constitution (2019)

In 2019, the Transitional Military Council (TMC) issued the Constitution document for the transitional period (Republic of Sudan 2019). Article 42/2 stated that 'all rights and freedoms, which included in human rights instrument that ratified by Sudan are integrated part of the document'. Item (2) of same article added that all rights and freedoms in this document will be regulated by law in a manner so as to ensure that those rights and freedoms are not restricted unless it is necessary as in a democratic society.

Article 55 addresses privacy and stipulates that abuse of a person's privacy is prohibited. Interference in one's personal and family life, correspondence and home is not allowed except as prescribed by law.

Combat Information Technology crimes Law of 2018

Sudan's 2007 **Combat Information Technology crimes** (Cybercrimes Law) was revised in 2018 and amended in 2020 to increase the severity of available punishments. According to article 5/1/A of the Cybercrimes Law 2018 (amended 2020), the court will imprison for five years anyone who intentionally accesses websites that are owned by others without permission, which constitutes a safeguard to protect the right to privacy. It is worth mentioning that the punishment was previously two years (before the 2020 amendment). Article 5/1/B adds that the court will imprison for six years anyone who intentionally accesses information systems owned by others, or

deletes, destroys, discloses, copies, uses or changes that information. (The punishment term was three years prior to the 2020 amendment.)

Chapter 14 of the law, entitled Crimes Related to Moral and Public Order, criminalises the production, publishing, promotion, possession or storing of contents that breach moral and public order according to article (19). Moreover, article 22 criminalises using the internet to assault religions or their leaders. Article 20 adds prohibition of the online promotion of prostitution, indecent actions, and using applications to breach the moral and public order. Article 21 stipulates that it is considered a crime under this law to spread ideas, programmes, sayings or actions that breach 'the moral and public order'. However, there is no legal definition of 'moral and public order' or the actions considered acceptable within those terms, which leaves the law open to abuse.

Article 23/1 amended by law No. 14/2020 stipulated that the state will punish (with up to four years in prison or a fine or both) anyone who sets up or uses information and communication networks or other cyber means or applications to abuse the privacy of any person or interfere in his or her personal and family life through taking and publishing photos, reading and publishing messages, or spreading fake news. The lack of a clear definition of fake news and the legal criteria that would identify fake news give ground for surveillance practices and undermine human freedoms, particularly freedom of expression and opinion.

Article 23/2 states that the action described in 23/1 does not constitute a crime if it took place upon judicial decision, upon decision from public prosecution, or by 'competent authority'. Competent authority is not necessarily a judicial body, whereas it could be a security agency. Without a clear definition of moral and public order, the right of privacy is at risk of abuse. Lack of definition and legal criteria embody the state of legal uncertainty. The legal certainty principle as one of the rule of law indictors, simply refers to the fact that 'enforcement of legal norms in a given situation to be predictable, the incident legal norm to be easily to establish, its recipients to be certain a legal provision corresponding offense is applied, and not another one, and that it will be interpreted in a uniform manner' (Ciongaru 2016: 45). Sudan is not the only country that uses undefined words and reasons to justify and 'legalise' surveillance and breaches of the right to privacy. For example, article 25 of Egyptian cybercrime law No. 175/2018 uses the same strategy.

Communication and Post Regulation Law 2018

Without including a clear definition of 'national security' or what is considered a 'high interest of Sudan', article 6/J of the Communication and Post Regulation Law 2018 states that the purpose of the regulatory authority is to protect the national security and the high interest of Sudan in the field of ICT.

National Security Law 2010

According to the National Security Law 2010, amended by law No. 12/2020 (Republic of Sudan 2020), article 25 gives power to the National Security Agency to request any information, data or document and to retain it.

Under a previous article, the National Security Agency has a right to collect information and exercise surveillance legally. Moreover, the law did not provide any sort of guarantees that ensure the right to privacy; national security officers are not required in advance to provide any sort of justification for collecting data and using surveillance. Moreover, the law did not require any previous judicial review for such a request.

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

The previous sections give an overview of existing national laws that regulate surveillance practices, highlighting the key international conventions that Sudan is party to and has used to prohibit communications surveillance. This section uses the Declaration of Principles on Freedom of Expression and Access to Information in Africa (hereafter the African Declaration) (African Commission on Human and Peoples' Rights 2019) as a means to compare Sudanese law against a rights-based ideal approach in the practice of surveillance.

While principle 40 of the Africa Declaration states that 'Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information', it also states that 'Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies'. Although the Sudanese Constitution and the Cybercrimes Law emphasised the right to privacy, this is contradicted by article 25 of the National Security Law and Article 23/2 of the Cybercrimes Law, which enable the state to breach the right of privacy and permit surveillance practices. Therefore, Sudanese legislation is not in line with international standards that guarantee the right to privacy and the inviolability of personal life and communications.

In addition, principle 41 adds that 'States shall only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim'. In this regard, the African Declaration is aligned with the International Principles (EFF 2013). However, Sudanese legislation breaches the principle of legal certainty as it does not clearly stipulate the legitimate aims that allow the authorities to practice surveillance, and it does not set specific time periods for the validity of judicial orders and their expiry.

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

As addressed in previous sections, the principles of legality, legitimate aim, proportionality and transparency are key to ensure elimination of electronic surveillance. Article 4 of the UN Draft Legal Instrument set out principles to ensure that surveillance systems shall be authorised by law prior to use. The law shall identify the purposes and situations in which the surveillance system is to be used, and define the category of serious crimes and/or threats for which the surveillance system is to be used (legitimate aims). The principles argue that states should set up and promote procedures to ensure transparency about and accountability of surveillance data and non-surveillance data for surveillance purposes. Sections 3, 4 and 9 of this report illustrate that Sudanese laws regarding surveillance are not in line with the UN Draft Legal Instrument, specifically in terms of identifying the purposes and situations where the surveillance system is to be used and defining the legitimate aims of surveillance. Moreover, applicability of the emergency law constitutes a permanent legal challenge against the right to privacy and undermines any attempts to combat surveillance practices. Therefore, one key recommendation of this report is to amend Sudan's National Security Law to bring it in line with international standards.

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

According to principle 2 of the International Principles (legitimate aims), 'Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'. Principle 3 (necessity) states that 'Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights'.

As already noted, existing surveillance laws in Sudan do not include definitions or explanations of key legal terms such as reasonable grounds or legitimate purpose. According to the Paradigm Initiative (2019), the Sudanese Cybercrimes Law 'uses vaguely defined terms that help regulate the content produced and consumed online'. For instance, article 21 stipulates that it is considered a crime under this law to spread ideas, programmes, sayings or actions that breach 'the moral and public order'. However, there is no legal definition of 'moral and public order' or which acts would be considered contravening that order, which leaves the law open to abuse. Furthermore, article 23/1 amended by law No. 14/2020 stipulates that the state will punish (with up to four years in prison or a fine or both) anyone who spreads fake news. Again, there is no clear definition of what constitutes fake news, which gives ground for surveillance practices and undermines human freedoms, particularly freedom of expression and opinion. In the same context, without a clear definition of 'national security' or what is considered a 'high interest of Sudan', article 6/J of the Communication and Post Regulation Law 2018 states that the purpose of the regulatory authority is to protect national security and the high interest of Sudan in the field of ICT.

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

According to the EFF (2014), the International Principles stipulate that 'States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties…' In addition, 'States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual'. Furthermore, the duty of governments to deter unlawful surveillance by way of criminal and civil sanctions reflects the requirements of international human rights law to protect individuals from breaches of their privacy, not only by the state but also by private individuals (EFF 2013).

Although Sudanese law prohibits surveillance except where authorised by judicial decision, and emphasises the right to privacy, and article 23/1 (amended by law No.14/2020) prohibits the breach of the privacy of others, article 25 of the National Security Law gives national security officers the powers to use surveillance. It is difficult to assess legal safeguards in the context of surveillance because – according to article 25 – there is no requirement for judicial permission in advance. Moreover, the lack of clear criteria, list of reasons, justifications and cases that allow issuance of a judicial decision to permit surveillance reflects the fact that existing safeguards are not sufficient and have not eliminated surveillance practices. In addition, the lack of clear definitions of key terms, legal criteria and definitions of acts that would constitute a crime under the Cybercrimes Law make legal procedures and actions unpredictable.

In conclusion, the way of drafting Sudanese law, the included legal guarantees in Sudanese laws, and using ambiguous terms are not operating to ensure elimination of surveillance practices.

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

Although Sudan is party to the ICCPR and other human rights conventions that protect the right to privacy, the Sudanese legal framework lacks a specific law to protect and guarantee the right to privacy. Despite the Constitution prohibiting abuse of personal privacy, and the Cybercrimes Law clearly prohibiting abuse of an individual's privacy (which is considered a crime), the Cybercrimes Law gives the investigating authority the right to issue orders that could abuse a person's right to privacy without providing specific grounds for doing so. Moreover, as already noted, the National Security Law gives national security agencies the power to access information without judicial review and without oversight by an independent authority.

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

All surveillance is a violation of the right to privacy. However, some surveillance is legal. Legislation can define the legitimate aims of surveillance, such as the prevention of serious crimes. These legal boundaries refer to the legality of practices that constitute a restriction on human rights, and aim to protect human rights against arbitrary practices by the state (EFF 2013).

The lack of specific criteria for justifying the issuance of a judicial order and thereby permission for surveillance constitutes a breach of privacy. Lack of clear definitions of 'moral and public order' as justifications for breaching the right to privacy and lack of reasons for authorised national security officers to collect personal information reflect the difficulties in assessing whether existing surveillance practices in Sudan are legal, necessary and proportionate. The Sudanese state has absolute discretionary power to assess the necessity and proportionality of surveillance practices without any sort of judicial review.

10. How has surveillance law played out in court in Sudan?

No surveillance law cases were identified by the literature search for this report. There was one court decision related to an internet shutdown, which is reviewed here because of its potential relevance to strategic litigation on surveillance within the Sudanese judicial system.

In 2019, the Court of Appeal in Khartoum, in its decision in the case recorded under No. (M1/ASM/520/2019-/520/2019 م س أ/1م), upheld the decision of the lower court and required the mobile internet service provider (El Zain) to reconnect the communication and internet services to the plaintiff. The appellant stated that the shutdown of internet and communication in Sudan was upon verbal request from the Telecommunication Regulatory Authority on the basis of threats to national security. The court stated that the internet shutdown occurred after the success of the Sudanese revolution, which led to removing Al-Bashir's regime on 11 April 2019, successfully arguing that there was no national threat at that time. The court found that the internet shutdown was in breach of Article 39/1 of the suspended Sudanese Constitution, which stipulated that each citizen has the unrestricted right to freedom of expression and to receive and spread information.

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

Although Sudanese law includes basic effective legal provisions that could play a role in protecting the right to privacy, the same law includes other provisions that compromise its effectiveness.

The lack of personal data protection law in Sudan is a major gap in privacy protection. Moreover, article 25 of the National Security Law, which gives the National Security Agency the right to request personal data and keep a copy of it, opens the door to secret and arbitrary surveillance practices.

Article 23/2 of the Cybercrimes Law does not specify the legitimate aims that allow the investigating authority or judicial bodies to breach privacy and carry out legitimate surveillance practices. This constitutes abuse of the principle of legal certainty.

In light of Chapter 14 of the Cybercrimes Law, entitled Crimes Related to Moral and Public Order, definitional clarity is needed. The lack of a legal definition of what constitutes 'fake news' or 'public and moral order' leaves the law open to abuse.

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

Parliament and legislators

- Amend article 23/2 of the Cybercrimes Law by specifying the 'legitimate aims' that investigating agencies can use to request permission to conduct targeted surveillance.
- Ensure respect for the principle of legal certainty by clearly defining in law the parameters of national security, fake news and moral and public order.
- Require prior authorisation from a judicial authority for all surveillance. Require a judge to test requests for reasonable grounds, legality, necessity and proportionality.
- Amend the National Security Law and specify the cases that give the National Security Agency the right to collect information, which should be upon judicial order in advance.
- Adopt a data protection law.

Non-governmental organisations (NGOs)

- Build the capacity of lawyers on digital rights to enable them to conduct strategic litigation in surveillance practices and right to privacy, and encouraging them to challenge surveillance motivation laws before constitutional courts.
- Establish a coalition between NGOs working on digital rights to engage in the policy-making process and communicate with decision-makers to advocate for improvements to existing laws and practices and bring them in line with the International Principles.
- Use international and regional human rights mechanisms to change existing policies, practices and laws.

Academia and research centres

- Produce a policy paper focusing on surveillance legislation gaps and suggest changes required to ensure the right to privacy.
- Conduct comparative analysis of experiences of other countries in the region to explore applicable experience and solutions that could apply in Sudan.

References

Abubkr, L.E. (2014) 'Sudan', in A. Finlay (ed), ***Global Information Society Watch 2014: Communications Surveillance in the Digital Age***, APC and Hivos (accessed 10 August 2021)

AFEX (2019) ***AFEX Annual Report on the State of Internet Freedom in Africa - 2019***. Accra: African Freedom of Expression Exchange (accessed 13 August 2021)

African Commission on Human and Peoples' Rights (2019) ***Declaration of Principles on Freedom of Expression and Access to Information in Africa*** (accessed 10 August 2021)

Ali, A.M. (2020) **'Sudan 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 10 August 2021)

Amnesty International (2010) ***Agents of Fear: The National Security Service in Sudan***, London: Amnesty International (accessed 10 August 2021)

Ciongaru, E. (2016) **'Constitutional Law Connotations of Legal Certainty in the Rule of Law'**, *Fiat Iustitia* No. 1/2016: 43–50

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

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) **'Mapping Hacking Team's "Untraceable" Spyware'**, *The Citizen Lab,* 17 February (accessed 10 August 2021)

OpenNet Initiative (2009) ***Internet Filtering in Sudan*** (accessed 10 August 2021)

OpenNet Initiative (2004) ***A Starting Point: Legal Implications of Internet Filtering*** (accessed 10 August 2021)

Paradigm Initiative (2019) ***Digital Rights in Africa Report 2019***, Lagos: Paradigm Initiative (accessed 10 August 2021)

Republic of Sudan (2020), Khartoum: Ministry of Justice, Government of the Republic of Sudan, *Official Gazette* Issue No. 1904, 13/7/2020

Republic of Sudan (2019) The Constitutional Document for the Transitional Period, *Official Gazette,* Issue No. 1895, 3/10/2019

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

University of Minnesota, Human Rights Library (no date) ***'Ratification of International Human Rights Treaties – Sudan'*** (accessed 10 August 2021)