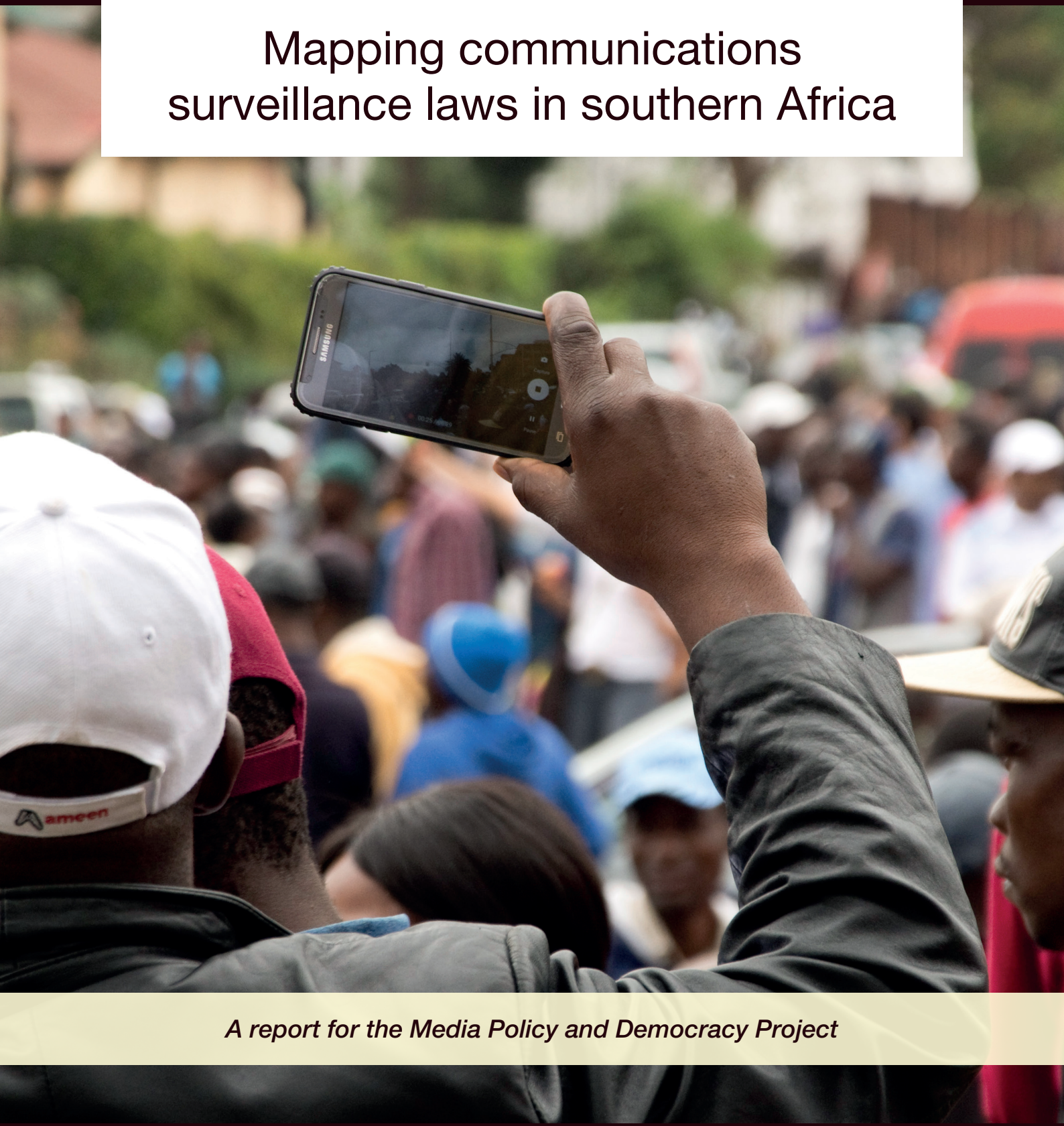
A Patchwork for Privacy

Mapping communications surveillance laws in southern Africa



A report for the Media Policy and Democracy Project

Murray Hunter and Admire Mare

A Patchwork for Privacy

Mapping communications surveillance laws in southern Africa

A report for the Media Policy and Democracy Project

This research attempts to map out basic features of communications surveillance laws in 12 southern African countries, to assess the extent to which the legal frameworks for digital surveillance meet or fall short of international best practice. This is an attempt to address an information gap in surveillance studies, which tend to focus more on the global north. As the digitisation of African societies progresses, understanding and mapping out the frameworks for communications surveillance is an increasingly important part of assessing the climate for democratic engagement in these countries.

Perhaps unsurprisingly, the research reveals a dispiriting picture. Across the region, governments appear to be exercising intrusive spying powers with insufficient limitations or safeguards. In particular, communications metadata (information about a person's communications, rather than the content of their communications) is left with little legal protection. In several countries, the state's surveillance powers are not subject to approval by a judge, eschewing the most basic standard for independent oversight. In some parts of the region, governments have exercised these intrusive powers with no legal framework in place; others have legal frameworks full of overlaps, conflicts and blind spots. Above all, irrespective of strengths or weaknesses in legal framework, a pattern emerges across the region: states have used their surveillance powers for anti-democratic purposes.

In the context of global debates on privacy and the growing realisation of the importance of communications privacy in democratic participation, the aim of this research is to contribute to an understanding of the basic features of the interception laws for each country in southern African. This can form the basis for ongoing research and democratic reforms, to build a better foundation for communication rights in the region.

Murray Hunter and Admire Mare

May 2020

The authors wish to acknowledge the assistance of Professor Rui Verde, Professor Jane Duncan, the African Legal Information Institute (African LII), and the Collaboration on International ICT Policy in East and Southern Africa (CIPESA).

Cover image by Graham van de Ruit

Contents

1 Introduction

The 2013 revelations by Edward Snowden of global mass surveillance programmes by the US government and its allies ignited urgent questions on the need for greater protection of human rights and democratic freedoms in an era of unprecedented potential for mass digital surveillance. A 2014 report by the UN High Commissioner for Human Rights found that:

> *Deep concerns have been expressed as policies and practices that exploit the vulnerability of digital communications technologies to electronic surveillance and interception in countries across the globe have been exposed. Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure.*[1]

The realisation that the world is caught up in a 'dragnet' has 'accelerated a necessary debate about the future of Internet policy and the importance of data protection in an increasingly globalised world interconnected by digital infrastructures.'[2]

The urgency of this 'necessary debate' is in no small part because of the potential for communications surveillance to disrupt and violate not only the right to privacy but also other basic civil liberties: invasions of privacy may also have a chilling effect on political activism, public protest and debate, and investigative journalism – and thus on 'the overall character of critical democratic engagement, dissent and the ability of marginalised people to challenge those with power.'[3]

1 UN High Commissioner on Human Rights. 'The Right to Privacy in the Digital Age', June 2014. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc
2 Pohle, J. and Van Audenhove, L. (2017). Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. *Media and Communication* 5(1): 1–6.
3 Right to Know Campaign. (2016). The Surveillance State: Communications surveillance and privacy in South Africa. Retrieved from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf

The situation has been worsened by a tendency for lower legal safeguards for the privacy of communications 'metadata' than for communications 'content',[4] reflecting an assumption about the non-sensitivity of metadata that is increasingly discredited. Underscoring the sensitivity of information about a person's communications, the UN High Commissioner for Human Rights found that:

> *The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.*[5] [emphasis added]

Among other reform efforts, in 2013 international civil society bodies and experts developed the 13 'Necessary and Proportionate' principles, introduced to the United Nations Human Rights Committee to offer a guiding framework to align modern communications surveillance laws and practices with human rights protections.[6] These 13 principles would serve as conditions under which any state may exercise the power to intercept a person's communications: broadly speaking, that the use of such powers must be regulated by a law; be restricted to the prevention of only the most serious offences and threats to human life; that the use of such powers must be authorised by an independent judge; that basic transparency and public oversight measures must be in place; and so on.

However, it is not at all clear that such efforts have yielded progressive reforms. Existing legislation and practices in many countries have not been updated to address the threats and challenges of communications surveillance in the digital age.[7] Elsewhere, draconian cybercrime laws have been passed or new policy measures to defeat encryption are in the works – often with the stated purpose of national security, online safety, or combatting heinous online crimes. Scholars have also raised concerns over the state of accountability and transparency mechanisms in most countries.[8] In Europe, Australia and the United States, tweaks to legislation and oversight have already been made, but their privacy credentials are uncertain at best.[9]

---

4 Most interceptions laws create a distinction between communication 'content' and communication 'metadata'. 'Content' might be understood as what is said in a call or message, and metadata would be any information about the communication – an index of who communicated with whom, when, where, over what devices, and so on.

5 UN High Commissioner on Human Rights. 'The Right to Privacy in the Digital Age', June 2014. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc

6 International Principles on the Application of Human Rights to Communications Surveillance, 2013. https://necessaryandproportionate.org/

7 La Rue, F. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/ HRC/17/27 (Geneva: United Nations General Assembly, Human Rights Council, 2011), 12, Retrieved from www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC .17.27_en.pdf

8 See Simcox, R. (2015); Surveillance After Snowden: Effective Espionage in an Age of Transparency. The Henry Jackson Society. Duncan, J. (2018). *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*. Johannesburg: Wits University Press.

9 Baker McKenzie. (2017). Baker McKenzie's 2017 Global Surveillance Survey. Retrieved from https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en

Shifting to the global South

While these questions have been subject to global policy debates, their focus has often been unevenly distributed; less attention is afforded to countries in the global South, and to those in Africa in particular. For example, among 39 jurisdictions profiled in the Global Surveillance Surveys by international law firm Baker McKenzie, just one is located on the African continent – South Africa.[10]

So what is the communications surveillance picture for African societies? Anecdotally, fears of invasive surveillance have become a more prominent feature of repression of dissent in a number of countries in the region.[11] The vast majority of African countries have adopted mandatory Subscriber Identification Module (SIM) registration, requiring all communications users to link their electronic communications to their legal identities. Although states that impose this policy usually justify it as a necessary measure to prevent crime, there is little evidence that SIM registration policies are effective in reducing crime.[12] In fact, SIM registration programmes have been criticised for enabling more pervasive systems of surveillance, as well as excluding marginalised groups from important civic spaces and social services.[13] The increased prominence of Chinese state-linked telecommunications companies in many African markets – often apparently acting as technical implementers for national government telecommunications and interceptions programmes – has sparked additional concerns about the geo-politics of digital surveillance.[14]

A recent academic survey found at least 25 African countries have enacted a law to authorise and regulate interception of communications – some placing these powers under the authority of a judge, others with the executive, and some taking a 'hybrid' approach where the authority is shared between the judiciary and executive.[15]

10 For comparison, the survey includes six countries from South America and ten from Asia.
11 See, for example, Freedom House (2019). 'Freedom on the Net'. Retrieved from: https://freedomhouse.org/report/freedom-net/
12 Jentzsch, N. (2012). 'Implications of mandatory registration of mobile phone users in Africa', *Telecommunications Policy* 36: 609.
13 Privacy International (2019). 'Africa: SIM Card Registration Only Increases Monitoring and Exclusion'. Retrieved from: https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion
14 See Mare, A. (2019) 'Facebook, youth and political action: A comparative study of Zimbabwe and South Africa'. A PhD dissertation submitted to the School of Journalism and Media Studies, Rhodes University, Grahamstown, South Africa; Media Policy and Democracy Project (2019). 'Drifting Towards Darkness: An Exploratory Study of State Surveillance in Post-2000 Zimbabwe'. Media Policy and Democracy Project. Johannesburg. Retrieved from http://mediaanddemocracy.com/
15 Mavedzenge, J. (2020). 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance'. *African Journal on Legal Studies* 1–35.

This research attempts to advance these discussions, by mapping out basic features of communications surveillance laws in 12 southern African countries. Drawing on key features of the 'Necessary and Proportionate' principles, it aims to assess the following features of the legal frameworks:

- Is there a law that regulates interception of communications and communication data?
- Does the law require judicial authorisation, for the police or intelligence agencies to intercept people's communications?
- Is the use of the law restricted to serious offences?
- Are those targeted for surveillance notified after the fact?
- Does the law give lesser protection to communications 'metadata' than to communications 'content'?
- Does the law provide for the retention of communications data (and for how many years)?
- What other forms of oversight does it provide for?
- Does the law require registration of SIM cards?

In each instance the authors have tried to answer as simply as possible. Following the logic of the 'Necessary and Proportionate' principles, in most categories a simple 'yes' or 'no' value has been applied to each finding (although these should not automatically be read as positive or negative attributes for each law). In some instances no simple answer is possible, due to ambiguities in the law or gaps between the law and what authorities do in practice. Nonetheless, as the summary table shows, the research reveals a dispiriting picture:

	Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
		Police	Intel					
South Africa	✓	✓	✓	✓*	✗†	✗	36 months	✓
DRC	✓	✓	✗	✗	✗	✗	✗	✓
Tanzania	✓	✗*	✗	✗	✗	✗	✗	✓
Angola	✓	✓	✓	✓*	✗	✗	✗	✓
Mozambique	✗*	✗	✗	✗	✗	✗	✗	✓
Malawi	✗	✗	✗	✗	✗	✗	✗	✓
Zambia	✓	✓	✓	✗	✗	✓	3 months	✓
Zimbabwe	✓	✗	✗	✗	✗	✗	6 months*	✓
Namibia	✓*	✓	✓	✗	✗	✗	✗	✗
Botswana	✓	✓	✓	✗	✗	✗	✗	✓
Lesotho	✓	✓*	✗	✗	✗	✓	36 months†	✗
eSwatini	✗	✗	✗	✗	✗	✗	✗	✓

NOTES

*Only access to content is restricted to serious offences. Metadata may be accessed for any offence

†Courts may overturn this

*Except using the terror law

*Restricted to offences with a maximum prison penalty of more than two years

*There is a law but it is deemed non-functional

*De facto – no clear legal provision

*There is a law but it is only partly implemented

*Some scope for warrantless access

†De facto – no clear legal provision

Figure 1: Summary of findings

Across the region, governments appear to be exercising intrusive spying powers with insufficient limitations or safeguards. In particular, communications metadata (information about a person's communications, rather than the content of their communications) is left with little legal protection. In several countries the state's surveillance powers are not subject to approval by a judge, eschewing the most basic standard for independent oversight. In some parts of the region, governments have exercised these intrusive powers with no legal framework in place; others have legal frameworks full of overlaps, conflicts and blind spots.

Above all, irrespective of strengths or weaknesses in legal framework, a pattern emerges across the region: states have used their surveillance powers for anti-democratic purposes.

As the digitisation of African societies progresses, understanding and mapping out the frameworks for communications surveillance is an increasingly important part of assessing the climate for democratic engagement in these countries.

2 South Africa

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓	✓	✓*	✗†	✗	36 months	✓

Notes: *Only interception of content is restricted to serious offences
†Courts may overturn this

Overview

South Africa's Constitution contains strong privacy protections and strict controls on the conduct of the police and intelligence services. However, there is significant evidence that state surveillance powers have been used to target journalists, government critics and dissident politicians.[16] At the time of writing, a legal challenge to South Africa's main surveillance law was before the Constitutional Court, after evidence emerged that state spies had intercepted the communications of a well-known investigative journalist.

Two main laws regulate the state's interception of communications and communication data: the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), and the Criminal Procedure Act 51 of 1977 (Section 205 of the CPA).

The RICA Act

RICA is the primary law that regulates the interception of communications in South Africa.

After years of criticism that RICA lacked vital privacy protections, in 2019 a High Court ordered several major revisions to the law.[17] At the time of writing, the Constitutional Court was expected to rule on the high court's findings, following a hearing in February 2020.

Judicial authorisation

In broad terms, RICA provides that law enforcement and intelligence agencies may only intercept a person's communications or metadata with the authorisation of a designated judge – for 'real-time' interceptions of communication, these applications must be put to a specially appointed 'RICA judge', whereas applications to seize historical metadata may be put to a High Court judge.

The Act does allow law-enforcement agencies to demand immediate access to someone's locational data without pre-approval of the judge, to prevent serious bodily harm or a life-threatening emergency.[18] These requests can be made orally, but the Act requires post-facto justification and notification to the RICA judge.

16 See Duncan, *Stopping the Spies*.
17 *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP) (16 September 2019).
18 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, sec. 7 and 8.

Restrictions on offences

Only relatively senior officials from law-enforcement and intelligence agencies may apply to intercept communications and communication data, and mostly only for the purposes of preventing or solving relatively serious crimes, including racketeering and gangsterism, violent crime, and terrorism. For the intelligence agencies, RICA also permits the interception of communication for broader intelligence-gathering grounds: threats to public health or safety, national security, or 'compelling national economic interests of the Republic'.[19]

Notification

In its current draft, RICA specifically prohibits any party from notifying a person that their communications have been intercepted.[20] In amaBhungane, the High Court struck this provision down after hearing argument that this provision had enabled surveillance abuses by ensuring that any people who are unjustly targeted for interception would have no way to protect their rights, because they would never know that their rights had been infringed. If the Constitutional Court upholds this finding, it would require the state to generally notify any person targeted for interception, unless the authorities can convince the RICA judge that there is an ongoing investigation or other reason to postpone notifying the target.

Metadata and retention

RICA requires every telecommunications or internet network to store all user metadata (which the Act calls 'communication-related information') for three years.[21]

In terms of its safeguards for access, RICA treats metadata as less sensitive than content, and historical information as less sensitive than 'real-time' information.[22] In terms of safeguards, the bar is lower for law-enforcement interceptions of metadata than for content, and lower still for requests in terms of RICA for historical metadata.[23]

19 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, sec. 16(5).
20 RICA, sec. 41.
21 RICA, sec. 30(2)a(iii).
22 'Real-time' is defined as any communication or metadata occurring contemporaneously or within the last 90 days.
23 Hunter, M. (2020). 'Cops and Call Records: Policing and metadata privacy in South Africa', Media Policy and Democracy Project, Johannesburg, 12. Retrieved from http://mediaanddemocracy.com/

Reporting and oversight

RICA requires the designated judge to submit annual reports to Parliament's intelligence committee,[24] which generally include a total number of interception warrants approved each year. However, when these reports finally become public, they have generally been found to lack the necessary detail and consistency required for public oversight.[25]

South African intelligence laws provide two forms of oversight for the intelligence services: a Parliamentary committee, which meets behind closed doors, and the Inspector General of Intelligence, a civilian ombud who can investigate complaints of misconduct or criminality in the intelligence services.[26]

SIM registration

RICA requires SIM card registration.[27]

Criminal Procedure Act

Section 205 of South Africa's Criminal Procedure Act includes a subpoena mechanism that is widely used by law enforcement to seize communications data. Using Section 205, a police officer may approach a magistrate to secure an order for a communications service provider to hand over the call records or metadata associated with a particular phone number or device.[28]

This serves as a parallel route for the authorities to access communication data which bypasses any safeguards contained in RICA. While metadata requests in terms of RICA may only be sought to investigate relatively serious offences and threats to national security, and only by relatively senior officials, metadata requests in terms of Section 205 of the Criminal Procedure Act can be made by a wide category of law enforcement officials, with sign-off from the most junior magistrates, for any offence. While the RICA judge must make an annual report which includes a total number of interception warrants issued, the hundreds of judges and magistrates issuing 'Section 205' subpoenas are not required to undertake any reporting on their work.[29]

24 RICA, sec. 60; Intelligence Services Oversight Act 40 of 1994, sec. 3(i)iii.
25 Duncan, *Stopping the Spies*, 93.
26 Intelligence Services Oversight Act.
27 RICA, sec. 39.
28 Criminal Procedure Act, sec. 205.
29 Hunter, 'Cops and Call Records', 13.

Above all, investigative research and freedom of information requests to service providers show that the Criminal Procedure Act is used exponentially more often than RICA to access metadata – while the RICA judge issues fewer than a thousand warrants per year in total, the courts issue as many as a thousand section 205 metadata orders per week.[30]

30 Hunter, 'Cops and Call Records', 13.

3 Democratic Republic of the Congo

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓	✗	✗	✗	✗	✗	✓

Overview[31]

The right to privacy is protected in Article 31 of the Democratic Republic of Congo's Constitution – but media freedom groups have expressed grave concerns that the government has engaged in invasive surveillance of its critics, in addition to its use of internet censorship and periodic state-directed internet shutdowns.[32]

The Framework Law 13/2002

The DRC's Framework Law 13/2002 regulates state interception of communications.

The law provides that telecommunication operators and their staff are required to respect the confidentiality of communications,[33] and prohibits any form of surveillance on citizens' communication, even by security agents, without prior authorisation from the General Prosecutor.[34]

The law generally requires judicial oversight in the conduct of communications surveillance, mandating the Attorney General to nominate a magistrate who will authorise security agents' requests to intercept and monitor telecommunication services.[35] This magistrate is expected to submit a comprehensive report to the Attorney General.

However, the law also allows exceptional circumstances where the Internal Affairs Minister may grant interception orders, on request of the Defence Minister and Head of the Intelligence Services.[36]

Although the law contains language guaranteeing security and privacy online, its use of vague terms may leave room for abuse. For example, it provides that the privacy of a person's communications 'can be infringed only by the public authority, when needed for public interest as described in the law'.37 The Act does not define its concept of 'public interest'. Nor does it define the similarly vague terms in Article 55 of the Act, which states that the Attorney General may only order interception of communications for the purposes of 'necessities of information motivated by the need to uncover the ultimate truth in a judicial affair'.[38]

31 The authors acknowledge research by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) from which the translations of DRC's statutes is drawn.
32 CIPESA (2016). State of Internet Freedom in Democratic Republic of the Congo 2016. Retrieved from https://cipesa.org/?wpfb_dl=234
33 Article 53 of the Framework Law 13/2002.
34 Article 54 of the Framework Law 13/2002.
35 Articles 57 and 58 of the Framework Law, cited in CIPESA, 2016.
36 CIPESA, 2016.
37 Article 53 of the Framework Law, 2002.
38 Article 55 of the Framework Law, 2002.

The grounds on which interception may take place are also extremely broad – aside from national security, interception may be authorised to prevent criminality and 'organised hooliganism', as well as protection of essential elements of DRC's 'scientific, economic and cultural potential.'[39]

The Law 14/2002

The Law 14/2002 governs the operations of the DRC's telecommunications regulator, known as ARPTC. The Act grants the right for the government, specifically the legislature, to 'conduct site visits, conduct investigations and studies, and collect all the necessary data' from telecommunication service providers.[40] It also explicitly authorises the government to 'collect all necessary data' from telecommunications companies when needed.[41]

The 2015 Ministerial Order

A Ministerial Order issued in 2015 enforced mandatory SIM card registration in the DRC. The move resulted in government-imposed disconnections of unregistered SIM cards. The Order requires telecommunication companies to send data collected about subscribers' identities to government services before deleting it from their database.[42] In short, this allows the government to engage in communications surveillance without taking the route of acquiring consent from an independent judicial officer. Like the Framework Law of 2002, some of the key terms like 'national security' and 'a judicial case' are vague, opening up opportunities for government abuse.

New Bills before Parliament

At time of writing, several Bills are before the DRC parliament which would amend the state's interception powers. These are the Telecommunications and ICT Bill (which is aimed at updating the Framework Law 013/2002 on Telecommunications), as well as the e-Transactions Bill, and a law pertaining to the telecommunications regulator. Similar to the old laws, these news bills have been critiqued for containing vague words such as '*public interest*', '*disruption of public order*', '*ultimate truth*', and '*national security*'.[43]

39 CIPESA, 2016.
40 Open Net Africa (2019). DR-Congo parliament urged to pass laws that support citizens' rights. Retrieved from https://www.opennetafrica.org/dr-congo-parliament-urged-to-pass-laws-that-support-citizens-rights-online/
41 CIPESA, 2016.
42 CIPESA, 2016
43 CIPESA, 2016.

4 Tanzania

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✗ *	✗	✗	✗	✗	✗	✓

Note: *Judicial authorisation is only required for interceptions related to terrorism

Overview

In Tanzania, the right to privacy is recognised under the Bill of Rights of the 1977 Constitution.[44] Article 16 of the Constitution also calls for the enactment of a law that stipulates how privacy rights may be protected or interfered with by the government.

Despite these progressive constitutional provisions, over the past few years the country has enacted a series of draconian laws relating to communication privacy and cybersecurity, which have contributed to a chilling effect of online freedom of expression.[45] A survey of its interceptions framework shows that the Tanzanian authorities have given themselves wide discretion to intercept citizens' communications and metadata, usually without independent oversight or judicial authorisation.

But while Tanzania's laws do provide for the state to intercept people's communications from network operators and ISPs, as of 2017, it appears no such protocols were actually in place: the Vodafone group stated in a series of annual disclosures that it had not implemented the technical requirements necessary for lawful interception of 'content' in Tanzania, on the basis that the state had not laid out regulations for this.[46]

However, its annual disclosure reports do provide a summary of demands by law-enforcement agencies for users' communications data (i.e. metadata):

Vodacom Tanzania disclosures of government requests for communications data		
Period	**Requests**	**Year-on-year change**
2013/14	n/a[47]	–
2014/15	933	–
2015/16	2,137	129%
2016/17	4,158	95%

44 The Constitution of the Republic of Tanzania, 1977.
45 CIPESA (2014). 'State of Internet Freedoms in Tanzania 2014'. Retrieved from https://www.opennetafrica.org/?wpfb_dl=18
46 Vodafone PLC, Country by Country Disclosure of Law Enforcement Assistance Demands (2014, 2015, 2016, 2017). Retrieved from: https://www.vodafone.com/content/index/about/sustainability/operating-responsibly/human-rights/digital-rights-and-freedoms.html
47 Vodafone's 2014 report stated that it had received over 90,000 metadata requests in Tanzania in the previous year, but it withdrew this number in subsequent reports, stating that it was the result of a technical error in its system. It did not supply a corrected figure for that year.

Tanzania Intelligence and Security Service Act

The governing law of Tanzania's intelligence services, the Tanzania Intelligence and Security Service Act, does not have specific provisions relating to interception, but simply provides that Tanzania's intelligence service has a duty to collect intelligence on activities 'that may on reasonable grounds be suspected of constituting a threat' to Tanzania's security.[48] No judicial oversight is provided. It is unclear if the Tanzanian authorities invoke this statute for interceptions, but it is included in the Vodafone group's global disclosure of interception laws relating to its operations.[49]

The Electronic and Postal Communications Act of 2010

The Electronic *and* Postal Communications Act (EPOCA) of 2010 governs all electronic and postal communications and telecommunications in Tanzania – and appears to be the primary interceptions law of Tanzania. It is administered by the Tanzania Communications and Regulatory Authority (TCRA).

The interception provisions contained in the EPOCA are not clearly spelled out, but only inferred: section 120 makes it an offence for a person to interception communications except if they have lawful authority under the EPOCA or any other law.[50] Section 120 gives the power to adjudicate warrants to the Director of Public Prosecutors.

A set of investigation regulations issued alongside the Act reportedly provide for the head of Tanzania's intelligence services and the Director of Criminal Investigations to intercept users' communications, upon a warrant being issued by the Inspector General of Police.[51] Thus, interceptions are not subject to judicial approval.

Regulations on Telecommunications Traffic Monitoring System Regulation

In 2013, the Tanzanian authorities issued regulations that allow the telecommunications regulator to install a traffic-monitoring system capable of collecting communications metadata in real-time, with no apparent judicial approval. This provision is found in the Electronic and Postal Communication (Telecommunications Traffic Monitoring System) Regulations –

48 Tanzania Intelligence and Security Service Act, sec. 14.
49 Vodafone Group Plc, Digital Rights and Freedoms. Legal Annexe: Overview of legal powers, 2016.
50 Vodafone Group Plc, Digital Rights and Freedoms. Legal Annexe: Overview of legal powers, 2016.
51 Sinda, A.A. and Kamuzora, F. (2018). 'Privacy and data protection in Tanzania, part 1', Bowmans Law. Retrieved from: https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

providing for the regulator to install a traffic monitoring system capable of collecting call detail records. While the stated purpose of these provisions is to assess network operators' compliance with regulations, there is a clear risk of abuse.[52]

The Prevention of Terrorism Act of 2002

While interceptions under Tanzania's Electronic and Postal Communications Act can take place without a judge's oversight, judicial authorisation is required for interceptions under Tanzania's terrorism law. According to section 31 of the Prevention of Terrorism Act of 2002, a police officer may, with the approval of the Attorney General, apply to a judge to intercept communications in an investigation of a terrorist offence. Thus, only in terrorism-related investigations does a court rule on whether or not the authorities may intercept a person's communications.

SIM card registration

There is a biometric SIM card registration requirement in Tanzania, which is required by the Electronic and Postal Communications Act of 2010. Section 84 of the EPOCA requires network operators to submit details of all subscriber numbers and devices to a central register, held by the telecommunications authority, to be updated monthly.

52 Vodafone Group Plc, Digital Rights and Freedoms. Legal Annexe: Overview of legal powers, 2016.

5 Angola

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓	✓	✓*	✗	✗	✗	✓

Note: *Restricted to offences with a maximum prison penalty of more than two years

Overview

Despite strong constitutional protections for privacy and other civil liberties, Angola has a dismal record on digital rights.[53]

As one scholar noted: 'In Angola there is a big difference between what is written and what is in practice applied. You´ll find a robust framework defending privacy and fundamental rights guaranteed by judicial intervention that in daily life is not respected.'[54]

Thus, while Angola's laws generally require any interception of communication to be approved by a court, these may be regarded with scepticism.

This research noted very little Anglophone scholarship on communications privacy and surveillance in Angola. However, human rights monitors have observed serious concerns and suspicions among journalists and pro-democracy activists that the Angolan security structures wield covert spying powers against them.[55] This includes evidence that government agencies deployed spyware against a leading investigative journalist, and reports that Chinese telecommunications firms have helped build state interception capacity that is not subject to oversight or checks and balances.[56]

Nonetheless, a brief overview of the legal framework follows.

Constitution

Article 34 of Angola's Constitution provides for the protection of communication privacy, which authorities may only interfere with by decision of a judge:

34.1. The confidentiality of correspondence and other means of communication is inviolable particularly of postcards, telegraphic, telephone and telematics.

34.2. Only by decision of a competent judicial authority under the terms the law, public authorities are allowed to interfere in correspondence and in other private media.[57]

53 See Gwagwa, A. 'Digital Media: An emerging repression battlefront in Angola?' November 2017. Retrieved from https://www.cipit.org/images/downloads/Angola-Report-Final.-1.pdf

54 E-mail interview with Professor Rui Verde, 7 May 2020.

55 Freedom House, 2019. ' Freedom on the Net 2019: Angola'. Retrieved from: https://freedomhouse.org/country/angola/freedom-net/2019

56 Freedom House, 2019. ' Freedom on the Net 2019: Angola'.

57 Constitution of the Republic of Angola, sec. 34. Translation by Rui Verde.

Criminal law

Article 210 of Angola's Code of Criminal Procedure, or Código de Processo Penal, also provides that interception of communications must be authorised by a judge.

The parameters of this power are found in a 2014 statute, the Regulatory Act for Searches and Seizures (Lei Reguladora das Revistas, Buscas e Apreensões), article 17 of which provides for seizures in postal and telecommunication services.[58] The conditions for seizure of any telecommunications correspondence are that it must be ordered by a judge, if the judge has reason to believe that it relates to a crime for which the seizure is 'of great interest to prove the crime or to discover the truth'.[59] In terms of this law, the authorities may not intercept a person's communications for relatively minor offences – the suspected crime must carry a maximum prison sentence of more than two years.[60]

The National Security Act

Angola's National Security Act of 2002 (Lei Segurança Nacional) also requires judicial intervention for wiretapping in national security operations. The Act spells out a fairly wide national security mandate for Angola's various security and policing structures: to produce intelligence to protect security, human life and dignity, national sovereignty, public peace, and to prevent various security threats such as terrorism, sabotage, espionage, and drug trafficking.[61]

This mandate serves as the general context in which the authorities may use national security powers in terms of the Act, including wiretapping. However, article 2 provides that those powers must be used in line with human rights and freedoms protected in the Angolan legal framework.[62]

Article 24 of the National Security Act provides that wiretapping must be authorised by a senior judicial figure (the 'Counsellor Judge of the Criminal Chamber of the Supreme Court'[63]), and that any decision on a wiretap must be issued within three days of a request by the national security structures. A wiretap warrant issued in terms of the Act is valid for up to 45 days, after which it must be renewed.[64]

58 Law 2/14 (Lei No. 2/12), article 17.
59 '*...se revista de grande interesse para a prova do crime ou para a descoberta da verdade.*' Law 2/12, article 17.1(c).
60 Law 2/12, article 17.1(b).
61 Law 12/02, article 1.3.
62 Law 12/02, article 2.
63 '*...Juiz Conselheiro da Câmara Criminal do Tribunal Supremo*', Law 12/02, article 24.1.
64 Law 12/02, article 24.3.

Article 25 of the Act provides for the establishment of data processing centres ('Centro de Processamento de Dados') whose purpose is limited to defense of the democratic state and prevention of crime.[65] However, the scope and functioning of data processing centres is not spelt out in law and any role in interception of communications is unclear.

In terms of oversight, the Act provides for the security structures to report annually to the National Assembly, which also has the power to appoint a supervisory body.[66]

Metadata provisions

These laws do not appear to create a clear distinction between communications content and metadata. This research was unable to identify any provision in Angolan law that spells out how long communications metadata should be stored.

Notification

The laws do not provide for post-surveillance notification, except in instances where an investigation results in charges being produced and a case going to trial.[67]

SIM registration

The Angolan government enacted mandatory SIM card registration in 2014 via executive decree, which was fully enforced in 2016.[68]

65 Law 12/02, article 25; article 27.
66 Law 12/02, article 31.
67 Interview with Dr Verde.
68 Decree 20/14, Retrieved from http://www.inacom.gov.ao/registo/decreto.html

6 Mozambique

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✗*	✗	✗	✗	✗	✗	✗	✓

Note: *There is a law but it is deemed non-functional

Overview

According to the Constitution, all citizens are entitled to the protection of their private life and have the right to honour, good name, reputation, protection of their public image and privacy.[69]

Notwithstanding this, investigative reports have alleged that the Mozambican government engages in monitoring of e-mails and internet traffic of members of opposition political parties, and with capacity and support from the state of China.[70] Unlike many jurisdictions, interceptions in the Mozambican context do not require prior judicial authorisation.

Decree No. 33/2001

This Decree states that network providers must cooperate with the authorities regarding the legal interception of communications. However, as of 2017 the Vodafone group reported that no law or decree had established a clear process for such interception to take place, and said it had not had any requests or involvement in state interception on its networks.[71]

The Telecommunications Law

Article 68 of the Telecommunications Law (Law No. 8/2004 of 21 July) states that the secrecy of a user's communications is guaranteed except in cases of criminal law and in the interests of national safety and the prevention of terrorism, criminality and organised delinquency. By inference, the state assumes its right to access communications and communications metadata.

However, it does so without any judicial oversight, and seemingly without meaningful limitation, restriction or proportionality.

It would appear that government demands for metadata are made through the Telecommunications Law; the Vodafone group does not disclose how many requests for communications metadata it received from the government of Mozambique, stating that that it has been 'unable to obtain guidance' from the government on whether disclosure of this information was prohibited by law. Although no such law has been identified, Vodafone's

69 The Constitution of the Republic of Mozambique.
70 Global Voices. (2016). The Government of Mozambique is 'Spying its citizens', According to @Verdade, 16 May 2016. Retrieved from https://advox.globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/
71 Vodafone Group Plc, Digital Rights and Freedoms. Legal Annexe: Overview of legal powers, 2016.

decision not to report on it metadata handovers suggests that Mozambique's interceptions practice is subject to de facto non-disclosure.

SIM card registration

Like its neighbours, Mozambique requires mobile phone users to register their SIM cards, through Decree No. 18/2015 of August 2018.

7 Malawi

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✗	✗	✗	✗	✗	✗	✗	✓

Overview

The right to privacy is protected in the Constitution of Malawi, which explicitly includes protection from 'interference with private communications, including mail and all forms of telecommunications'.[72] On the face of it, there is no law that explicitly regulates state interception of communications in Malawi. This does not appear to have stopped the Malawian state from seeking to intercept people's communications, however; state surveillance of communication is 'strongly suspected'[73], and the Malawian government has procured technology that appears to be capable of intercepting massive amounts of call-related data from telecommunications networks.

The passing of two controversial laws in 2016 – the Electronic Transactions and Cyber Security Act (the E-Transactions Act) and the Communications Act – sparked concerns about state surveillance, but neither explicitly deals with communications interceptions.

The E-Transactions Act

The E-Transactions Act is a wide-ranging cybersecurity law, with provisions that regulate e-commerce, domain registration, child pornography, spamming, online harassment, and regulation of encryption services, as well as restrictions on online content. The Act provides for the appointment of 'cyber inspectors', who may apply to a court for a search warrant to inspect and collect any record held by any information system, pertaining to any investigation.[74] Clearly, this could include communication data, at least in legal interpretation if not in reality.

The E-Transactions Act states that no person can 'gain unauthorised access to, or intercept, or interfere with data', meaning any information in electronic form. However, the Act provides that the Minister of Communications may issue regulations on specific conditions where intercepting or interfering with data may be permitted.[75]

However, if this Act is meant to regulate the interception of communications, there is a lot missing. State interception of communication is not listed among the objectives of the Act.[76] The Act does not distinguish between communications data and any other data that might be held by an internet service provider. It is also entirely silent on telecommunications networks,

72 Constitution of the Republic of Malawi, sec. 21.1a.
73 Freedom House, 'Freedom on the Net 2019: Malawi'. Retrieved from: https://www.freedomonthenet.org/country/malawi/freedom-on-the-net/2019
74 ETCSA, sec. 70.
75 ETCSA, sec. 84.
76 However, the Act's objectives do include ensuring that users are 'protected from undesirable impacts of information and communication technology, including the spread of pornographic material, cyber-crime and digital fraud' and safeguarded from 'fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of information and communication technology.' (E-Transactions Act, Sections 3(b) and (c).

even though telephony and mobile networks enjoy many more subscribers in Malawi than internet networks.[77]

The Communications Act

The Communications Act also makes it an offence to intercept communications 'without lawful authority under this Act or any other written law',[78] and prohibits service providers from disclosing the contents of electronic messages 'other than in accordance with this Act'[79] – but provides no procedures on how such disclosure could be in accordance with the Act.

Mandatory SIM registration was enforced through the Communications Act; Malawi's communications authority reportedly disconnected unregistered numbers after a September 2018 deadline.[80]

The Communications Act also mandates the Malawian communications authority, MACRA, to establish electronic monitoring of all communications services to ensure they comply with their licenses, but explicitly prohibits such a system from being used for 'monitoring actual content of communication, network traffic or for any other purpose other than its [license] monitoring mandate'.[81]

Like the E-Transactions Act, the Communications Act does not appear to meet the basic test of providing legal regulation to intercept communication, in that it provides no clear procedures for the state to do so.

MACRA's 'Spy Machine'

However, there is significant evidence that the Malawian state does assume the right to intercept users' communication in the absence of a law.

This spilled out in a long-running scandal surrounding Malawi's communications regulator, over a technological procurement known as the Consolidated ICT Regulatory Management System (CIRMS) – commonly referred to as 'the spy machine.'[82]

77 In 2017, fewer than 14% of Malawians had internet access while 44% had mobile phone subscriptions; this dropped to 39% the following year, presumably due to disconnection of unregistered SIMs. See: ITU Country ICT Data. Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
78 Communication Act, sec. 176(1) and (2).
79 Communication Act, sec. 177.
80 Freedom House, 'Freedom on the Net 2019: Malawi'. Retrieved from: https://www.freedomonthenet.org/country/malawi/freedom-on-the-net/2019
81 Communications Act, sec. 167.
82 Nyasa Times, 'Malawi to roll out 'spy machine'', 24 January 2018. Retrieved from: https://www.nyasatimes.com/malawi-roll-spy-machine/

According to news reports, the regulator purchased the system in 2011 from a US firm for a reported US$ 6.8 million, saying it was necessary to monitor the performance of ICT networks. However, it emerged in an ensuing legal challenge that the device was capable of intercepting call-related data from telecommunications services providers in real time – and had been acquired specifically for that purpose.[83] The regulator insisted that this data was needed to monitor the amount of traffic on companies' networks to ensure they were not under-declaring revenue.[84]

Although the system was blocked by several court challenges, Malawi's Supreme Court ultimately set aside various injunctions by the lower courts, clearing the way for MACRA to implement the CIRMS system in full.[85] There is no reported evidence of it having been employed for the purposes of communications interception, however.[86]

Over the course of the litigation, the license agreements between MACRA and each of the network operators came before the court – revealing that interception of communication was a condition of each operator's license. In its initial ruling, the High Court cited a clause appearing in all networks' operator licenses:

> The Licensee shall not monitor or disclose the contents of any communication conveyed as part of a public telecommunications service except:
>
> **a.** to the extent necessary for the purpose of maintaining or repairing any part of the network used to provide the service or monitoring the Licensee's quality of service;
>
> **b.** when requested to do so by a person authorized by law or by an order of the court;
>
> **c.** if so requested by a competent authority for the maintenance of national authority.[87]

It is not clear when this provision first appeared in operator licences, but this indicates that, in the absence of a law, the Malawian government has still asserted its right to intercept users' communication.

83 Judgment in *Kimu v Access Malawi Limited and Others* (Commercial Case No. 54 of 2011) [2012] MWCommC 1 (02 May 2012), 5.
84 Nyasa Times, 'Malawi to roll out 'spy machine'.
85 Kainja, J. 'Privacy and personal data challenges and trends in Malawi', CIPESA report, September 2018. Retrieved from: https://cipesa.org/?wpfb_dl=300
86 Freedom House, 'Freedom on the Net 2019: Malawi'. Retrieved from: https://www.freedomonthenet.org/country/malawi/freedom-on-the-net/2019
87 *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012)

8 Zambia

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓	✓	✗	✗	✓	3 months	✓

Overview

Article 17 of the Constitution of Zambia protects the right to privacy, which is framed as a protection against a search of person or property.[88] Though Zambia does have a law that regulates interception of communication, there is a dearth of information about the government's surveillance capabilities, and how it wields them. Work by journalists and human rights organisations points to evidence that the state has sought to expand its spying powers and turn these against its critics; among other things, the Israeli-made spyware Pegasus has been detected in Zambia, and Zambian officials were among the potential clients exposed in leaked e-mails of the Italian surveillance firm Hacking Team.[89] The government's relationship with Chinese telecom Huawei has also roused suspicion; an investigation by the Wall Street Journal gave detailed accounts of Huawei technicians' intercepting digital communication or providing real-time tracing of suspected criminals, opposition politicians and dissident bloggers for Zambian authorities.[90]

The Electronic Communications and Transactions Act

The Electronic Communications and Transaction Act (ECA) of 2009 governs interception of communications – as well as a wide range of other communications matters, including registration of telecommunications and internet service providers, content regulations, standards of service, cybercrime and data protection.

Judicial oversight

To intercept communications, the Act requires law enforcement officers to apply for an order to a judge, and also get the permission of the Attorney General.[91] Zambian authorities may intercept communications for any offence, regardless of seriousness.[92]

This order may require a service provider to intercept or retain communication, or allow the law enforcement officer to install a device to intercept specific communication, among other things.[93] The order is valid for three months, and authorities may apply to renew the order; the judge may decide the length of a renewal.

88 Constitution of Zambia, 1991 (amended 2016), Act 17.
89 Freedom House, 'Freedom on the Net 2019: Zambia'. Retrieved from: https://www.freedomonthenet.org/country/zambia/freedom-on-the-net/2019
90 Wall Street Journal, 'Huawei technicians helped African governments spy on political opponents'.15 August 2019. Retrieved from https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
91 ECA, sec. 66.
92 ECA, sec. 66(3).
93 ECA, sec. 65(3).

The Act also contains provision for life-or-limb emergencies, whereby a police officer orders service providers to intercept communications without a warrant, and submit all documents to a judge after the fact for review. An officer can use these emergency procedures where a person has done bodily harm to themselves or others (or threatened to do so), or 'has caused or may cause damage to property.'[94]

The state may also get remote access to a computer via a warrant,[95] which could be interpreted as a provision to allow state 'hacking'.

Illegal interception of communication is punishable with up to 25 years imprisonment.[96]

The provisions of the Act apply equally to Zambia's police and intelligence services, as well as to other agencies: the Anti-Corruption Commission and the Drug Enforcement Commission.

Notification

The Act does not provide any notification procedure for users whose communication is intercepted. Regulations handed down in 2011 also prohibit service providers from disclosing information about methods of interception, or the identities or services being targeted.[97]

Metadata protections

The Act does not distinguish between communications 'content' and 'metadata'. The Act refers to various kinds of communication, which at times have overlapping definitions or which aren't defined, including 'call-related information', 'content', 'electronic communication', as well as 'wire' communication, and 'data messages'. However, there is no clear difference in the protections and procedures that apply to these different forms of communication. Separately, the regulations refer to 'communication-related information', which is not defined. In South Africa's interception law, 'communication-related information' has a similar definition to 'call-related information' in Zambia's law, which poses the possibility that its inclusion in Zambia's regulations is the result of a haphazard adaptation of South African legislation.

94 ECA, sec. 67(4).
95 ECA, sec. 83(1).
96 ECA, sec. 64.
97 Regulations, sec. 42(4).

Metadata retention

Regulations issued for the implementation of Zambia's communications and interception law state that communications-related information must be held for at least 90 days.[98] There does not seem to be a maximum period for their retention.

Oversight

The Electronic Communications and Transaction Act provides that decisions relating to interceptions could fall to an Office of the Public Protector, which has powers to investigate alleged abuses of power or wrongdoing by any public body or official.[99, 100] The Public Protector has the equivalent powers of a High Court Judge, but there are some limitations on the office's powers, including that it may not investigate any complaint relating to a member of the Parliamentary Service or Judicial Service, or which is criminal.[101] The amended Constitution also provides for a Police Public Complaints Commission, which may receive complaints about police action, although it is not clear if this could include decisions relating to interceptions. In any case, this body has recommendation powers only.

SIM registration

The Zambian government issued regulations for mandatory SIM registration in 2011, invoking powers from the 2009 Information Communication Technologies Act.[102] In 2012, Zambian investigative journalists reported that the state may be compiling information about registered SIM cards into a central database.[103] The same regulations required the registration of all mobile devices,[104] although this policy has yet to be implemented; a 2019 policy paper issued by ZICTA made clear that it still wishes to create a database of registered devices.[105]

98 The Electronic Communications and Transactions General Regulations, Statutory Instrument No 71 of 2011, sec. 47(1).
99 Constitution of Zambia (Amendment), No 2 of 2016.
100 The Commission for Investigations Act, Chapter 39 of the Laws of Zambia.
101 Constitution of Zambia (Amendment), sec. 245.
102 Information and Communication Technologies (Registration of Electronic Communication Apparatus) Regulations, 2011, sec. 12.
103 Freedom House, 'Freedom on the Net 2019: Zambia'. https://www.freedomonthenet.org/country/zambia/freedom-on-the-net/2019
104 Information and Communication Technologies (Registration of Electronic Communication Apparatus) Regulations, 2011, sec. 11.
105 Zicta, 'Consultation paper on the introduction of a new electronic communications equipment repository and registration regime', May 2019. Retrieved from: https://www.zicta.zm/Downloads/publications/EnhancedSIMandIMEIRegistration.pdf

9 Zimbabwe

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✗	✗	✗	✗	✗	6 months*	✓

Note: *De facto – no clear legal provision

Overview

There has been extensive reporting on evidence of extrajudicial surveillance by repressive state apparatuses in Zimbabwe.[106] Local and international investigative reports have documented e-mail snooping and other surveillance methods to target opposition party activists and human rights defenders.[107]

Zimbabwe has a number of laws and statutory instruments on communications surveillance. These generally fall far below international best practice because of the power they invest in the executive to authorise its own surveillance activities in the absence of judicial oversight, and because they fail any test of proportionality.

Interception of Communications Act (ICA) of 2007

The Interception of Communications Act (ICA) of 2007 is Zimbabwe's primary communications surveillance law. The law grants interception powers to the Central Intelligence Organisation (CIO), the Police and the Zimbabwe Revenue Authority (ZIMRA), and Zimbabwe's defence intelligence agency. Rather than requiring authorisation from a judge, the Act provides that a cabinet minister may issue interception warrants – either the Minister in charge of communications, or any other that the President designates.[108]

The grounds on which the Minister can authorise interception of communication is broad – including for a wide range of violent crimes, property crimes, and organised crime, as well as for vaguely worded national security-related information gathering, relating to 'an actual threat to national security or any compelling national economic interest' or 'a potential threat to public safety or national security'.[109]

An interception warrant issued by the Minister is valid for three months, and can be renewed for another three months with relative ease.[110] There does not appear to be any limit on how many times an interception warrant can be renewed.

Section 9 of the Act also places intermediary liability on mobile operators and internet service providers (ISPs) compelling them to install the hardware and software required for the state to

106 Media Policy and Democracy Project (2019). Drifting Towards Darkness: An Exploratory Study of State Surveillance in Post-2000 Zimbabwe. Media Policy and Democracy Project. Johannesburg. Retrieved from http://mediaanddemocracy.com/

107 The Standard, 'Shutting down the citizens: Forget your privacy you are under surveillance', 26 January 2020. Available: https://www.thestandard.co.zw/2020/01/26/shutting-citizens-forget-privacy-surveillance/

108 Interception of Communications Act (Act 6 of 2007), sec. 6.

109 ICA, sec. 6.

110 ICA, sec. 7.

carry out interception, as well as to store call-related information (metadata) for an unspecified period.[111] (Section 12 of the ICA states that POTRAZ, the communications authority, must issue a directive within two months of the Act's commencement specifying interception protocols and the period for which communication-related information must be stored, but no such directive is publicly available. Court records suggest the metadata retention period could be six months: in a 2017 criminal case in the Harare High Court, this was cited as the period for which a network provider stored customer call records.[112]

In terms of protections for privacy and other rights, the Interception of Communication Act leaves much to be desired. However, it does have two provisions which in theory offer some protection that is missing from many of equivalent laws in the region: the requirement for destruction of intercepted material and a requirement for some form of administrative reporting about the interceptions system.

In the former case, Zimbabwe's intercept law requires that any intercepted communication should be destroyed 'as soon as possible after it is used for the purposes of this Act'.[113]

In the latter case, the law provides for some form of administrative review of the executive warrant system – section 19 of the Act states that the Minister who issues interception warrants should submit an annual report to the Attorney General which provides particulars of all warrants issued in that year. The Attorney General has the power to make recommendations on the implementation of the Act, which the Minister must comply with.[114] While this falls far short of the oversight standards proposed through the international 'Necessary and Proportionate' principles, this provision may suggest one opportunity to bolster democratic oversight of communications interceptions in Zimbabwe – notably, that civil society or watchdog organisations could call for the publication of any such reports, should the relevant minister have submitted them.[115]

The Criminal Procedure and Evidence Act (CPEA)

As in several neighbouring countries, the Zimbabwean authorities have explicitly invoked search and seizure powers in ordinary criminal law to access phone records, thereby applying an even lower bar to accessing communication data. Section 50 of the Criminal Procedure

111 Section 12 of the ICA states that POTRAZ, the communications authority, must issue a directive within two months of the Act's commencement specifying interception protocols and the period for which communication-related information must be stored, but no such directive is publicly available.
112 *S v Bonyongwe* (HH 193–17 CRB 18/16) [2017] ZWHHC 193 (01 March 2017).
113 ICA, sec 17.
114 ICA, sec 19.
115 See The Right to Privacy, Interception of Communications and Surveillance in Zimbabwe, Retrieved from http://crm.misa.org/upload/web/the-right-to-privacy-interception-of-communications-and-surveillance-in-zimbabwe.pdf

and Evidence Act provides for the police to search and seize any item or document for any criminal matter, if granted a warrant by a magistrate or judge.[116] However, in the event that an officer has reasonable grounds to believe that a warrant would be granted if one were applied for, and that any delay in getting a warrant would prevent the search or seizure, he or she may conduct a search or seizure without a warrant.[117] There appears to be no requirement to consult or even to notify a court after the fact. Section 54 of the Act goes even further, providing that a police officer may enter any premise without a warrant to inspect documents or other records, make copies of them, or interrogate a person there. The only requirement is that the officer deems it 'necessary for the purpose of investigating or detecting an offence'.[118]

The Harare High Court has explicitly upheld that the police could use this provision to access a person's call records, in a 2011 case in which opposition politician Tendai Biti tried unsuccessfully to block police from accessing his and others' phone records.[119] The police were investigating allegations that Biti abused his power as Finance Minister, by granting certain favours to a ministry employee with whom he was said to be romantically entangled. As part of its investigation – which came at a time when Zimbabwe's security cluster was reportedly seeking to discredit Biti and other opposition leaders[120] – the police had invoked section 54 of the CPEA to seize phone records for three numbers associated with Biti from Econet Wireless. 'Out of an abundance of caution' (to quote the court) the police did also secure a warrant from a magistrate. In dismissing Biti's challenge to this, a high court judge found that Section 54 of the CPEA 'quite clearly authorizes the police to obtain without warrant the required information [phone records] not only upon reasonable suspicion that a crime has been committed but also for purposes of detecting crime.' The court also found that where a search warrant has been issued, the law provides no appeal.[121]

SIM card registration

The Zimbabwean government introduced compulsory SIM card registration in 2013, through the controversial Statutory Instrument 142/2013 as well as Statutory Instrument 95/2014. The latter also provided for Zimbabwe's telecommunications authority to create a centralised database where all subscriber information would be held, although it is unclear if the authorities have implemented this.[122]

116 Criminal Procedure and Evidence Act (Chapter 9:07), sec. 50.
117 Criminal Procedure and Evidence Act (Chapter 9:07), sec. 51.
118 CPEA, sec. 54. This provision applies to any place except a private dwelling.
119 *Biti v Majuta and Others* (HC 6608/11) [2011] ZWHHC 156 (12 June 2011).
120 Global Witness, 'Financing a Parallel Government? The involvement of the secret police and military in Zimbabwe's diamond, cotton and property sectors', June 2012. Retrieved from: https://www.globalwitness.org/documents/10522/financing_a_parallel_government_zimbabwe.pdf
121 *Biti v Majuta and Others* (HC 6608/11) [2011] ZWHHC 156 (12 June 2011).
122 Statutory Instrument 95 of 2014, sec. 8.

10 Namibia

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓*	✓	✓	✗	✗	✗	✗	✗

Note: *There is a law but it is only partly implemented

Overview

Article 13 of Namibia's constitution protects the right to privacy – but similar to its neighbours, Namibia has a number of controversial clauses in its laws that impact on communications privacy. There is also evidence that the state engages in communications surveillance despite the fact that key provisions in its main interceptions law (the Communications Act of 2009) are not yet in operation.[123]

Other concerning practices include the push by the government for the roll-out of the Single Internet Gateway system; calls for mandatory SIM card registration; the alleged existence of interception centres; the absence of judicial authorisation and transparent oversight mechanisms over the intelligence agencies; and a proposed cybercrimes bill.[124]

The Namibian Central Intelligence Service (NCIS) Act, 1997

The NCIS Act regulates, among other things, the interception powers of Namibia's intelligence service. The Act sets out clear safeguards to prevent abuse and uphold the right to privacy.

In terms of the NCIS Act, if the Namibian intelligence service wishes to intercept a person's communications over a telecommunication network, it must first obtain a High Court warrant, on presentation of evidence of a serious threat to national security.[125] The request must be specific to a type of communication and target, limiting the risk of conducting untargeted 'fishing' expeditions. It is not clear, however, how metadata and the intrusive powers of the intelligence services are regulated in the current legislation.

The Communication Act of 2009

The Communication Act of 2009 includes provisions regulating the interception of telecommunications in Namibia. However, a decade after the Act as promulgated, these provisions are still not in force according to the Namibian government.[126]

Part 6 of the Act provide for the establishment of interception centres, staffed by members of the Namibian intelligence services, for the purposes of combating of crime and protecting national security. The Act stipulates that before an intelligence operative performs any function

123 Mare, A. (2019). 'Communications Surveillance in Namibia: An Exploratory study'. Media Policy and Democracy Project. Johannesburg, 14.
124 Mare (2019). 'Communications Surveillance in Namibia', 19.
125 Article 25, Namibian Central Intelligence Service (NCIS) Act, 1997.
126 Mare (2019). 'Communications Surveillance in Namibia'.

in relation to interception or monitoring of telecommunications, he or she must obtain consent of a judge.

However, as these provisions have yet to come into force, it is not clear where the state's legal powers of interception are drawn, and with what oversight and regulation; this is in light of evidence that the country has acquired a variety of smart technologies such as the International Mobile Subscriber Identity (IMSI) and other technologies.

Notification

The Communications Act does not provide for post-surveillance notification of users. It does not explicitly prohibit such notification, but, as the case is for the equivalent law in South Africa, the Namibian Act does prohibit any person involved in an interception from revealing information or doing anything that defeats the purpose of the interception.[127]

Criminal law

Court records in Namibia show that police investigators and prosecutors have drawn on cell phone records as evidence in criminal justice.[128] One likely possibility is that the authorities invoke section 205 of Namibia's Criminal Procedure Act to subpoena a suspect or accused person's phone records. The Namibian Act closely resembles the South African Act of the same name (it inherited the law from South Africa's statute books during South Africa's decades-long de facto rule over Namibia), and it may be that authorities use it in the same way to access communications data (see page 11). This study was not able to source any research on the legal means used by Namibian authorities to access phone records in criminal matters, but one interviewee echoed the understanding that police have used Namibia's Criminal Procedure Act.[129]

SIM card registration

SIM registration is not currently required in Namibian law, but the Namibian government has proposed to implement it in the future. This proposal has been endorsed by the ruling party.[130]

127 Communications Act 8 of 2006, sec. 75(a).
128 See, for example, *S v Neidel and Others* (CC 21/2006) [2011] NAHC 232 (27 July 2011); *S v Hangombe* (CA 43/2012) [2012] NAHC 304 (23 August 2012).
129 Author's e-mail correspondence with Frederico Links, journalist, 14 May 2020.
130 Mare (2019). 'Communications Surveillance in Namibia', 19.

11 Botswana

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓	✓	✗	✗	✗	✗	✓

Overview

Similar to other jurisdictions, the Constitution of Botswana guarantees the right to privacy as outlined in section 9 (1): 'Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises.'[131]

The Constitution permits interference with a person's right to privacy on a wide range of grounds (albeit not all related to communications privacy): defence, public safety, public order, public morality, public health, town and country planning, mining activities, and census-taking.'[132]

Although little is known about the interceptions capabilities of Botswana, the security services are believed to have engaged in communications surveillance in the aid of the political battles of the ruling elite.[133] The Directorate of Intelligence and Security (DIS) and the Military Intelligence Unit (MIU) are also suspected to have acquired surveillance equipment from Israel in the run up to the 2014 general election, with capability to spy on both the internet and telephone conversations and jam radio and mobile signals.[134]

Disclosures by Orange, a global communications firm doing business in Botswana, give a limited snapshot of the lawful interception practices in Botswana:

Orange Botswana disclosures of government requests[135]			
Period	**Lawful interception**	**Communications data**	**Year-on-year change (on communication data)**
2014	0	340	-
2015	0	340	0%
2016	0	401	18%
2017	0	350	-13%
2018	0	579	65%

131 The Constitution of Botswana.
132 The Constitution of Botswana.
133 Balule, B.T. and Otlhogile, B. (2016). 'Balancing the right to privacy and the public interest: surveillance by the state of the private communications for law enforcement in Botswana. *Statute Law Review* 37(1): 19–32. Retrieved from https://mafiadoc.com/balancing-the-right-to-privacy-and-the-public-interest-_5b0836ed8ead0eee138b456f.html
134 Balule and Otlhogile (2016).
135 Orange SA, Transparency reports on freedom of expression and privacy protection (2014, 2015, 2016, 2017, 2018). https://www.orange.com/en/Group/Non-financial-reporting

Intelligence and Security Service Act of 2007

The Intelligence and Security Service Act (ISSA) provides for Botswana's intelligence services, the DIS, to intercept communications with the approval of a High Court judge or senior magistrate.[136] The authorities may seek an interception warrant to investigate any threat to national security, or for the intelligence services to fulfill any other part of their mandate.

However, the President is given wide discretionary powers under the ISSA to determine additional powers of the DIS and what would be in the national interest.[137]

Counter-Terrorism Act, 2014

The Counter-Terrorism Act allows for any officer of the Botswanan police, defence force or intelligence services to apply to a magistrate or judge for permission to intercept communications, for the purposes of investigating or preventing an act of terrorism.[138] An interception order made in terms of the Act lasts for 3 months, and can be renewed to a maximum of 6 months.

Telecommunications Act, 1996

Botswana's Telecommunications Act provides for the telecommunications industry to disclose customers' private communications to law enforcement agencies and the courts. Section 52 of the Act prohibits a person in the telecommunications industry to intercept a message or disclose the contents of a message, except "in connection with the investigation of any criminal offence or for the purpose of any criminal proceedings."[139]

The section makes no provision for a judge's warrant or subpoena, although it is possible that this is invoked using subpoena powers in Botswana's criminal law.[140]

SIM card registration

The Botswana Telecommunications Authority (BTA) introduced SIM card registration in September 2008.

136 Intelligence and Security Service Act of 2007, sec. 22.
137 Balule and Otlhogile (2016).
138 Counter-Terrorism Act, 2014, sec. 20; also cited in Mavedzenge (2020).
139 Telecommunications Act, 1996, sec. 52
140 Criminal Procedure and Evidence Act, 1939, sec. 54

12 Lesotho

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✓	✓*	✗	✗	✗	✓	36 months †	✗

Notes: *Some scope for warrantless access
†De facto – no clear legal provision

Overview

Lesotho's Constitution provides that every person is entitled to 'respect for his private and family life and his home.'[141] Lesotho has several laws pertaining to the lawful interception of communications and communication data. In general these require a court order, with several significant exceptions.

There is a serious dearth of research and analysis on communications surveillance in Lesotho. The Vodafone's global disclosure reports on law enforcement cooperation do include an analysis of the legal framework; however, this article identified several anomalies and omissions in that analysis.

It should be noted, while the laws do provide for real-time interception of communications, the Vodafone disclosures suggest that the technical capacity may not yet exist. In its 2016/2017 transparency report, the company said it had not received any demands from the Lesotho government to assist in intercepting communications. The report further stated that the company had not implemented the technical requirements necessary for lawful interception of 'content', on the basis that there is no law requiring it to do so.

In the same year, Vodafone Lesotho disclosed 3,376 requests for users' metadata[142] – representing an astonishing 592% increase in the four years for which such data is available.

Vodacom Lesotho disclosures of government requests for communications data		
Period	**Number of requests**	**Year-on-year change**
2013/14	488	–
2014/15	595	+ 22%
2015/16	1586	+ 167%
2016/17	3376	+ 113%

Vodacom Lesotho is one of four licensed network operators, and has a reported 80% share of the Lesotho mobile sector[143] – so while these numbers are not exhaustive, they do represent a large slice of the telecommunications sector.

141 Lesotho's Constitution of 1993, sec. 11.1.
142 Vodafone PLC, Country by Country Disclosure of Law Enforcement Assistance Demands (2014, 2015, 2016, 2017). Retrieved from: https://www.vodafone.com/content/index/about/sustainability/operating-responsibly/human-rights/digital-rights-and-freedoms.html
143 Vodacom Lesotho commercial feature, Africa Outlook, 30 October 2015. Retrieved from: https://www.africaoutlookmag.com/outlook-features/vodacom-lesotho

The Communications Act of 2012

The Communications Act of 2012, which provides for general regulations of Lesotho's telecommunications, postal and broadcast sectors, makes it an offence for any person to 'engage in interception or tracing of communications operations or messages unless authorised by a court of competent jurisdiction.'[144] Though the Act does not define any of the key phrases in that provision, a common-sense reading would be that a judge's approval is required for the interception of both content and metadata.

Telecommunications Authority Regulations of 2001

Regulations issued by the Minister of Communications prohibit telecommunications service providers from intercepting or sharing the contents of a message, or disclosing information about a customer, except in connection with the investigation of a criminal offence or for the purpose of criminal proceedings.[145]

Criminal Procedure and Evidence Act, 1981

Lesotho's Criminal Procedure and Evidence Act provides for any magistrate or judge to grant a police officer a search warrant to seize evidence in relation to any offence or suspected offence.[146] However, the Act also provides for a police officer (with the rank of warrant officer and above) to conduct a search without a warrant if they believe that by first obtaining the warrant it will defeat the purpose of the search.[147] While the Act provides that an officer who conducts such a search should then approach a magistrate with any evidence seized, there do not appear to be any safeguards or oversight mechanisms to prevent the abuse of this exception. Section 49 of the Act also allows a judge or magistrate to issue a subpoena for any document or other information or record that may be required as evidence in court proceedings.[148]

While the Act does not refer specifically to communications, it is among the laws cited by Vodafone as being applicable to its customers in Lesotho, suggesting that the Act has been invoked to get communications information, or could be.

144 Communications Act of 2012, sec. 44(1)f.
145 Regulation 32, Lesotho Telecommunications Authority Regulations, 2001.
146 Criminal Procedure and Evidence Act, 1981, sec. 46. The authors acknowledge AfricanLII.org and LesothoLII.org for publishing this Act online to assist our research.
147 Criminal Procedure and Evidence Act, 1981, sec. 47.
148 Criminal Procedure and Evidence Act, 1981, sec. 49.

Prevention of Corruption and Economic Offences Act, 1999

In the instance of corruption and economic crime, the authorities have special legal powers to seize information with no court order.

Through the Prevention of Corruption and Economic Offences Act, the head of Lesotho's anti-corruption agency may compel any person or entity to hand over information or documents, in the course of investigating a wide range of corruption and economic crime.[149] The relevant provisions are cited in Vodafone's schedule of relevant laws, suggesting that these provisions are invoked or at least interpreted to apply to communications services.

National Security Services Act, No. 11 of 1998

Although the Communications Act states that no interception may take place without a court order, the NSS Act grants a special exemption that allows the Minister of intelligence to authorise Lesotho's intelligence agency to intercept both communications content or any metadata held by a communications network. In these instances, such a directive does not require the oversight of a judge and does not necessarily need to be premised on a real and present threat to safety or security – interceptions can be ordered on any matter that is deemed to fall within the general functions or activities of the intelligence services.

This stems from section 26 of the NSS Act, which provides that the Minister may, on an application made by a senior-ranked intelligence officer, issue a warrant to enter or search any property, if the Minister deems it necessary to get information which '(a) is likely to be of substantial value in assisting the [national security services] in discharging any of its function; and (b) cannot be reasonably obtained by any other means'. Such a warrant is valid for six months and can be renewed by the Minister for another six months.

While this is followed by a separate provision on interception of communication, given the evidence that Lesotho's authorities and courts treat the seizure of metadata as an ordinary 'search', one can infer that this provision may be used to seize metadata. That Vodafone cites this provision in its list of applicable Lesotho laws supports this.

Section 27(2) of the NSS Act allows the Minister to issue a directive to intercept a particular communication or postal parcel, or to intercept all communications to or from a particular person or organisation on an ongoing basis. The Minister can issue such a directive if he or

149 Prevention of Corruption and Economic Offences Act, 1999, sec. 7(b) and 8(1).

she is convinced that it is necessary to investigate an offence or likely offence that threatens national security[150] or simply that it could yield information which 'has or could probably have a bearing on the functions of the Service'.[151] As with general search warrants issued under Section 26 of the Act, such a directive is valid for six months and can be renewed by the Minister for another six months.

Retention of communications data

Although – as the Vodafone reports make clear – the Lesotho government does regularly seek access to communications data for law enforcement purposes, there does not appear to be a legal requirement for service providers to store such data for any particular period. The only apparent requirement for network operators to store information about customer communications is in the four operator licenses issued by the Lesotho Communications Authority, which stipulates that the service provider must retain billing information for a period of 3 years for possible inspection by the Authority[152].

SIM card registration

At this time, SIM card registration is not a legal requirement in Lesotho.[153] However, in 2016 it was reported that the Lesotho Communications Authority was considering implementing mandatory SIM registration.[154]

150 Sec. 27(2)a.
151 Sec. 27(2)b.
152 Licenses granted by the Lesotho Communications Authority to LEC Communications (2015), Vodacom Lesotho (2001) and Tele-Com Mobile (2001), Retrieved from https://www.lca.org.ls/telecommunications/
153 Note: Lesotho has previously been listed in global research as one of the countries requiring SIM registration but this may be an error: there are no public details of such policy, and Lesotho network operators do not have any information advising consumers on how to register their SIM. See https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofOfID_R_WebSpreads.pdf
154 IT Web, 'Lesotho may introduce SIM card registrations', 22 June 2016. Retrieved from https://www.itweb.co.za/content/KrxP3jMBrYyMA2ye

13 eSwatini

Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
	Police	Intel					
✗	✗	✗	✗	✗	✗	✗	✓

Overview

The Constitution of eSwatini (known internationally as Swaziland until 2018) has an elaborate bill of rights which underscores the importance of freedom of expression. However, the monarchical government of eSwatini has a long track record of suppressing and interfering with civil liberties, including in the communications space. While much of that has taken the form of censorship, media reports have suggested the authorities have monitored private online communications without appropriate legal authority.[155] Civil society groups and human rights defenders have reported fears that the state has monitored their communications,[156] and it is suspected that the government monitors personal communications, social media and public gatherings – public or private criticism of the monarchy and other authorities is punishable under several statutes.[157]

The Electronic Communications Act of 2010

The Electronic Communications Act applies to the regulation of electronic communications. It does not regulate the content of messages transmitted through a communications network. The Act articulates the licensing requirements and procedures.

The Act writes an interception provision into the list of obligations created for network operators: '[licensees] must comply with all requirements related to legal interception as may be established under this Act or as a decision of the [eSwatini Communications] Commission'.[158] However, the Act provides no further detail for such a process, and there is no evidence that the authorities have issued any further directives to this effect.[159]

The Communications Commission Act of 2013

Since 2013, telecommunications and internet-based activities have been under the regulation of the eSwatini Communications Commission, in terms of the eSwatini Communications Commission Act.[160] While the Act does not provide specific measures for interception of communication data, it does give broad powers to the Commission to seize any data or

155 US Human Rights Report (2017). 'Country Reports on Human Rights Practices for 2015'. Retrieved from https://2009-2017.state.gov/j/drl/rls/hrrpt/humanrightsreport//index.htm
156 Human Rights Watch, 'World Report 2012: Swaziland, 2012'. https://www.hrw.org/world-report/2012/country-chapters/swaziland
157 Freedom House (2019). 'Freedom of the World 2019: Eswatini'. https://freedomhouse.org/country/eswatini/freedom-world/2019
158 The Electronic Communications Act of 2010, sec. 15(i).
159 No such directive appears on the list of regulations available on the Commission's website, and a research inquiry to the Commission sent on 28 February 2020 did not receive a response.
160 Gwagwa, A. (2015). 'Internet Censorship in Swaziland: Policy and Practice'. Retrieved from https://www.academia.edu/31116896/Internet_Censorship_in_Swaziland_Policy_and_Practice

information from network providers and internet service providers in pursuit of its mandate.[161] While generally this power is enforced through a request for information (for which non-compliance is an offence) the Act also empowers the Commission to physically access any premises under its mandate 'in situations which present difficulties, and in exceptional circumstances', to inspect or seize documents or data.[162] These search and seizure powers do not require a warrant or judicial approval.

Future legislation

As of a 2015 analysis, eSwatini did not have any legislation or regulation pertaining to cyber governance and activities. However, the Ministry of ICT has signalled that it will produce data protection laws and cyber-security legislation.[163]

SIM card registration requirements

In 2016, the government passed the SIM card registration Regulation, which gave birth to the VELA National Subscriber (SIM-CARD) Registration Project.[164]

161 Communications Commission Act of 2013, sec. 39.
162 Communications Commission Act of 2013, sec. 40.
163 Gwagwa (2015).
164 Swazi Observer, 'MTN to switch off unregistered Sim Cards, 19 February 2019.

14 Conclusion

Put together, a dispiriting picture emerges of communications surveillance laws in the southern African countries surveyed here. The legal frameworks for interception in southern Africa fall far short of the standards proposed in the Necessary and Proportionate Principles.

Recent years have already seen a rush of problematic cyber laws in the region, often with worrying provisions on collection of users' digital data, invasive state powers, and troubling restrictions for online speech.[165] In several African jurisdictions, these were seemingly preceded by harsh anti-terrorism laws that presented similar problems.[166]

Missing laws

A basic requirement for ensuring that a state's interception powers are subject to appropriate safeguards is legality: that there is a law which regulates the use of these powers.[167]

However, several states in the region do not have working legislation that regulates the interception of communications. This research could not identify any such law in Malawi, for example, whereas in Namibia there is an interception law on the books, but its operative sections are not in force.[168] There is clear evidence, however, that these governments have still sought to intercept people's private communications in the absence of a law; by definition, such action is unlawful. Indeed, the example of telecommunications licenses issued by the government of Malawi shows that even in the absence of a governing law, a state may simply 'write in' their interception powers via secret agreements with communications services.

165 See, for example, Access Now, 'Room for improvement: Implementing the African Cyber Security and DataProtection Convention in Sub-Saharan Africa', December 2016. Retrieved from: https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf

166 Gwagwa A., and Wilton A.(2014). 'Protecting the Right to Privacy in Africa in the Digital Age' Privacy International. Retrieved from https://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf

167 See 'Necessary and Proportionate' Principles, https://necessaryandproportionate.org/

168 Mare (2019).

It was not possible to find licensing agreements from all countries in the region for this research, but the Malawi example suggests that details of those agreements are relevant to a study of communications interception in the region. The interception powers of the eSwatini government seem to be nearly as thinly provisioned; in the absence of detailed procedures for interception, the state's surveillance power is simply written into the legal obligations of network providers.

Overlapping and conflicting laws

Where states do have laws that regulate their surveillance powers, this research often found a patchwork of overlapping and at times contradictory laws. As a result, safeguards for privacy created in one interception law might easily be circumvented through another. This is the case, for example, in South Africa, Lesotho and Tanzania, where the procedures in the national interception law run parallel to search and subpoena powers contained in ordinary criminal law, which seem to serve as a parallel avenue for authorities to access communication data. Many of the national legal frameworks in the region also create parallel standards and procedures for the police and intelligence agencies, so that one arm of the state is subject to a certain set of standards (such as they are) while another arm is not. These themes – lack of protections for metadata and lack of judicial oversight on intelligence – will be discussed further below.

Lack of proportionality in laws

Among those states that do have a law to regulate their interception powers, these laws typically lack any semblance of proportionality, in that they do not attempt to restrict the use of invasive powers to more serious crimes or security threats. Rather, these laws typically allow the state to resort to interception of people's communications for any law-enforcement or intelligence-gathering purpose. Among those countries surveyed, only South Africa's and Angola's interceptions law attempts to introduce some measure of proportionality, by restricting the use of interceptions to relatively serious crimes and security threats. But even these fall short: in South Africa, this restriction applies only to the real-time interception of the content of users' communication, whereas the state can access users' metadata with a subpoena for even minor offences. In Angola, the restriction is relatively mild: any criminal offence carrying a maximum sentence of more than two years' imprisonment could result in an interception of communications.

Gaps in judicial oversight

Generally speaking, these laws do require police to get the approval of a judge before intercepting a person's communication data – with several exceptions – but in most instances the intelligence services are given free rein: only the interception laws of Angola, Botswana, South Africa and Zambia require intelligence agencies to get judicial authorisation to conduct communication surveillance. Given the pattern across the region of state intelligence agencies interfering in domestic politics and public life, the lack of independent judicial controls of intelligence agencies' powers is a clear problem.

Lack of notification

The one commonality among all the surveillance regimes survey is that they lack user notification. In most jurisdictions this is the result of omission, in that the law is silent on notifying a person whose communication was intercepted – it is neither explicitly required or prohibited. Only South Africa, and possibly Zambia, appear to create a specific prohibition on notification. In the case of South Africa, the Constitutional Court may overturn this prohibition as part of its expected ruling in the amaBhungane case, which would then be replaced by a positive obligation on the state to notify people whose communications were intercepted. However, due to the limited scope of the case, if the Constitutional Court rules along those lines, that positive notification obligation would not apply in instances where the state seizes a person's communications metadata by ordinary subpoena.

Overall, lack of notification procedures indicate a key area where interception laws in the region lag behind international norms, where the trend is towards greater transparency. Post-surveillance notification has been held up as a vital safeguard to boost public oversight and narrow the window for abuses of surveillance power,[169] which would be particularly apt given the generally weak judicial and legislative oversight of state surveillance in southern Africa.

Weak protection for metadata

Privacy advocates have decried the tendency for interception laws to treat communications 'metadata' as less sensitive than 'content', and therefore subject to fewer protections. It is interesting to note that not all interception laws in the region explicitly follow that path;

169 See, for example, judgment in *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP) (16 September 2019).

the Zambian and Lesotho interception laws appear to provide that the same procedures apply for interception for all kinds of communication data, whether 'content' or 'metadata'. However, it should be noted that these procedures leave much to be desired.

More saliently, it would be premature to celebrate the privacy credentials of such a law, where lack of delineation between communications content and metadata may be the result of vagueness, rather than a conscious policy decision to protect privacy. Moreover, any protections in such a policy are meaningless when the authorities appear to use other legal avenues to access people's communication metadata; in South Africa, for example, the authorities are known to bypass the safeguards in the interceptions law to access phone records using ordinary search-and-seizure powers or subpoenas. Several other jurisdictions, including Lesotho and Namibia, appear to exercise similar powers through ordinary criminal law.

Metadata retention

A majority of the surveillance laws in southern Africa do not seem to require communication service providers to store their users' metadata for a specific period of time. Among the laws surveyed, only those in South Africa and Zambia appeared to require a minimum period of storage for law-enforcement purposes. However, there is little indication that this stems from a conscious policy decision to limit the storage of sensitive metadata; again, a lack of specificity may well be due to legislative fuzziness. The lack of protection is compounded by the fact that these laws generally do not provide a maximum period for retention either, leaving service providers to make up their own rules on data retention, or allowing states to write a period of retention into secret licensing agreements. This lack of specificity points to a broader lack of data protection policies in the region: although the SADC has adopted a model data protection law, within the region only Mauritius appears to have a data protection law in place. Several other countries (Angola, Botswana, Lesotho, Madagascar, South Africa) have passed a data-protection law but have yet to bring it into force.[170]

170 ALT Advisory, Data Protection Africa portal. https://dataprotection.africa/

Mandatory SIM registration

Most southern African countries have adopted a policy of mandatory SIM registration in the past decade; this is in keeping with the trend across Africa and the global South. Only two of the countries surveyed here, Namibia and Lesotho, did not have SIM registration policies in place – and both countries have indicated that they intend to adopt such a policy in the future. Although SIM registration is generally pursued on policing and national security grounds, researchers have found little empirical evidence that it lowers crime levels;[171] rather, it serves to enable a more pervasive surveillance system for those who use mobile services, and often excludes many others from those services.[172] When Malawi reached its SIM registration deadline in 2018, the rate of mobile subscriptions dropped by over 11% (from about 44 subscriptions per hundred people, to 30). In Zambia, the rate of mobile subscriptions dropped by nearly 10% between 2012 and 2014 (from about 73 subscriptions per 100 people, to 66).[173] In January 2014, the Zambian authorities boasted of disconnecting the owners of 2.4 million unregistered SIM cards.[174]

African states' commitment to SIM registration policies speaks to the long and challenging road ahead for reshaping the terrain for privacy in the region.

Patterns of abuse and unlawful spying

This assessment of legal surveillance regimes is complicated by one last common factor in each of the countries surveyed here: irrespective of their legal powers, each government faces significant evidence that it has been willing to break its own rules and use its spying powers for narrow and partisan interests. In this light, it is clear that the legal regimes for surveillance in southern Africa need dramatic overhaul, but this must be accompanied with fundamental changes in local climates for democracy, accountability and governance.

If such changes are to be possible at all, they must be built on knowledge and information. While the insights in this analysis draw on the findings of researchers, journalists, and civil society actors from across the region, these efforts only scratch the surface. As governments of southern Africa seek more advanced tools to expand their surveillance powers, it is clear that much more work is needed to piece together a proper understanding of how those powers are wielded, and what needs to be done to ensure greater protection for the right to privacy, freedom of expression, and democratic rights in Southern Africa.

171 Jentzsch, N. (2012). 'Implications of mandatory registration of mobile phone users in Africa'. *Telecommunications Policy* 36: 609.
172 Privacy International, 2019.
173 ITU Country ICT Data, Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
174 Lusaka Voice, 'Zambia switches off 2.4 million unregistered SIMs'. 6 February 2014. https://www.lusakavoice.com/2014/02/06/zambia-switches-off-2-4-million-unregistered-sims/

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit **mediaanddemocracy**.com for more information.

This report was supported by a grant from the Open Society Initiative for South Africa (OSISA)

OSISA
Open Society Initiative for Southern Africa