Compelled Service Provider Assistance for State Surveillance in Africa: **Challenges and Policy Options**

Policy Brief

March, **2023**

CIPESA

Table of content

Suggested citation:
CIPESA (2023), Compelled Service Provider Assistance for State Surveillance: Challenges and Policy Options

Introduction

In many Sub-Saharan countries, state surveillance, which generally refers to state measures to monitor and supervise activities of the population,[1] has become more pervasive and reliant on various digital technologies. The increasing communication surveillance, which entails the monitoring, interception, collection and retention of information through communication networks, undermines digital technology users' rights, including to privacy, and often places intermediaries in a position where they fail to comply with the United Nations Guiding Principles on Business and Human Rights (UNGPs).[2]

The right to privacy online is critical due to its intricate connection with, and its being a foundation for the protection and realisation of other rights, including the rights to freedoms of expression, information, assembly, and association. Anonymity while using digital technologies helps mitigate risks of surveillance and interception of private communication as well as retaliation by the state or other parties.[3] The fear of retaliation often forces individuals to withdraw from active participation in political and community affairs.[4]

Within the region, the key concerns around surveillance include the broad powers of state agencies to conduct surveillance, abuse of those surveillance powers, limited oversight and transparency over these surveillance activities.[5] For instance, across Africa, countries have enacted legislation compelling telecommunications service providers to embed technical capability within their systems to facilitate the interception of communications by state security agencies. Also, states have invested in software and hardware to facilitate surveillance and communication interception.

Also concerning are the strenuous and sometimes unclear demands by states on intermediaries, including to facilitate interception of communication, hand over communication data of their subscribers to state security agencies, and to take down content or shut down the internet. Others have adopted repressive legislation to control the spread of information on social media and to wantonly regulate internet intermediaries by placing undue liability on them for the content posted on their platforms.[6]

This policy brief examines how mandatory obligations on telecommunication intermediaries to facilitate state surveillance undermines their ability to comply with international standards including the UNGPs, and hamper users' rights. It draws on experiences from around Sub-Saharan Africa to illustrate how service providers are compelled through retrogressive policies and practices, to comply with state surveillance instructions.

The brief provides recommendations for governments, social media platforms, Internet Service Providers (ISPs), and civil society aimed at entrenching progressive principles in the implementation of lawful interception, empowering civil society actors to engage with technology companies to improve their human rights policies and practices, and informing efforts by businesses in awareness raising and advocacy for progressive technology governance.

1 *Ramasoota, Pirongrong, State Surveillance, Privacy and Social Control in Thailand, https://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/ftp03/NQ51914.pdf*

2 *United Nations Guiding Principles on Business and Human Rights, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf*

3 *Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications, https://www.ohchr.org/Documents/Issues/Opinion/Communications/PrivacyInternational.pdf*

4 *CIPESA, Effects of State Surveillance on Democratic Participation in Africa, https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf*

5 *Ibid.*

6 *CIPESA, Input for OHCHR report on the application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies, http://cipesa.org/wp-content/files/reports/Input-for-OHCHR-report-on-the-application-of-the-United-Nations-Guiding-Principles-on-Business-and-Human-Rights-to-the-activities-of-technology-companies.pdf*

Upsurge in State Surveillance in Africa

Surveillance is often regarded as important for maintaining security and safety[7] in both stable and unstable democracies, particularly where there are high levels of insecurity, such as the prevalence of terrorism, robberies, extra-judicial killings and general high crime rates.[8] Yet state surveillance is sometimes utilised as a tool for political control through instilling fear.[9]

Several countries across the continent have enacted laws that permit surveillance, mandate telecommunication intermediaries to facilitate the interception of communication, stipulate the mandatory collection of biometric data, limit the use of encryption, and grant law enforcement agents broad search and seizure powers, often with limited transparency or oversight.[10]

A 2021 analysis by the Africa Digital Rights Network (ADRN) found that privacy rights were being eroded in various African countries due to the introduction of new laws that expanded state surveillance powers; lack of legal precision and privacy safeguards in existing surveillance legislation; increased supply of new surveillance technologies that enable illegitimate surveillance; state agencies regularly conducting surveillance outside of what is permitted in law; impunity for those committing illegal surveillance; and insufficient capacity in civil society to hold the state fully accountable.[11] Similarly, research by CIPESA has found that surveillance laws continue to be implemented indiscriminately and in an opaque landscape with limited transparency and oversight by competent judicial authorities.[12]

The pervasive nature of state surveillance in Africa appears to be linked to the democratic regression and to the repression of digital rights. While the overall democracy deficit is growing across Sub-Saharan Africa, for the most part the countries that are cited for engaging in surveillance, particularly of human rights defenders (HRDs), journalists, and opposition politicians, are those where authoritarianism is on the rise. These countries also tend to implement other information control measures, have poor digital rights records, and weak accountability for human rights violations. Indeed, the 2021 and 2022 Democracy Index categorised 23 of the 44 African countries assessed as authoritarian, with only one being a full democracy.[13] Similar democratic regressions are documented in reports on *Freedom on the Net*; *Freedom in the World*; *World Press Freedom*, and the State of Internet in Africa 2021 report,[14] which highlights the effects of state surveillance on democratic participation in various African countries.

Various governments have invested in bolstering their surveillance capabilities, such as through the acquisition of software and equipment with capacity to conduct digital surveillance. They are also enforcing mandatory Subscriber Identification Module (SIM) registration laws that require all communications users to link their electronic communications to their legal identities for the alleged purpose of fighting cybercrime, and ordering telecom service providers to acquire systems that have backdoors to enable monitoring and interception of private communication.[15]

7 *See for instance, Jonathan Oram, "Balancing Surveillance between Needs of Privacy and Security: CCTV in Japan and England," 45; see also, Ambinder, Marc, and D. B. Grady. Deep State: Inside the Government Secrecy Industry. (John Wiley & Sons, 2013)*

8 *Welsh, Brandon C., and David P. Farrington. Making Public Places Safer: Surveillance and Crime Prevention. Oxford University Press, 2009.*

9 *Boyne, Roy, Post-Panopticism, https://www.tandfonline.com/doi/abs/10.1080/030851400360505*

10 *CIPESA, Effects of State Surveillance on Democratic participation in Africa, 2021, https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf*

11 *The countries which this research focussed on were Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan. See https://www.ids.ac.uk/news/state-surveillance-of-citizens-going-unchecked-across-africa/ .*

12 *CIPESA, Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa," and CIPESA, Mapping and Analysis of Privacy Laws and Policies in Africa, https://cipesa.org/?wpfb_dl=454*

13 *Economist Intelligence Unit, Democracy Index 2022, https://www.economist.com/graphic-detail/2023/02/01/the-worlds-most-and-least-democratic-countries-in-2022*

14 *CIPESA, State of Internet Freedom in Africa 2021 Report: Effects of State Surveillance on Democratic Participation in Africa, http://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf*

15 *A Patchwork for Privacy: Mapping communications surveillance laws in southern Africa, https://www.researchgate.net/publication/342078478_A_Patchwork_for_Privacy_Mapping_communications_surveillance_laws_in_southern_Africa, and CIPESA, State of Internet Freedom in Africa 2019: Mapping Trends in Government Internet Controls, 1999-2019, https://cipesa.org/?wpfb_dl=307*

Besides making large investments in new surveillance technologies, many African governments are also passing laws to expand their legal surveillance powers, while also conducting illegal surveillance. Research conducted in 2021 provides evidence of illegitimate state surveillance of journalists and academics in Egypt; of business rivals and politicians in South Africa; and of activists and lawyers in Sudan.[16] Indeed, the spread of surveillance technologies in Africa has thrust the continent into a critical inflection point, where it is torn between the increased capability to monitor citizens through widely available digital products, and protections for democratic norms and practices.[17]

Similarly, researchers have noted that many African states are deploying Artificial Intelligence (AI) surveillance technologies to monitor citizens for various purposes, but seldom in ways that are rights-respecting or particularly privacy-respecting.[18] A shared concern amongst the researchers is that AI surveillance technologies are not transparently procured or operated, and emphasis is placed on security or smartness of technology, without any human rights risk assessment or mitigation frameworks in place to protect people's privacy rights.

Why Compelled Service Provider Assistance is Problematic

Compelling service provider assistance is a key contributor to undermining users' privacy in Africa. The assistance rendered by intermediaries is used to facilitate internet disruptions, access to users' data with ease, content removals, decryption of users' encrypted data, and state surveillance.

In many countries in the region, compelled assistance undermines data privacy by enabling governments unfettered access to individuals' private data beyond prescribed limits. While legitimate law enforcement access may be necessary, this should be lawful and authorised by a court order outlining the nature, circumstances and extent of compelled service provider assistance. In any case, requests for compelled provider assistance must be for a specific period, targeted and limited to a particular case, and necessary and proportionate in the circumstances.[19] Moreover, there must be strong judicial and parliamentary oversight - which is lacking in many African countries.

Laws on *surveillance* and the interception of communications across the continent, including in Benin, Cameroon, Chad, Ivory Coast, Malawi, Mali, Niger, Nigeria, Rwanda, Senegal, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe mirror each other and require communication service providers to put in place mechanisms, including the installation of software, to facilitate access and interception of communications by state agencies.[20]

A key weak point in many countries' laws is that they restrict intermediaries and permit state agencies to conduct unwarranted surveillance. Such laws do not provide for sufficient judicial oversight or accountability mechanisms yet they place undue requirements on intermediaries, including compelling them to facilitate communication interception by state authorities, including in instances where there are no court-issued warrants authorising surveillance. Whereas laws in some countries already have regressive provisions that can be exploited to suppress freedom of expression and the free flow of information online, some governments have steadily weaponised them to target dissenters.

Moreover, state agencies in several countries can request for decryption of data held by intermediaries such as telecommunication and internet service providers, which exacerbates privacy concerns.

A worrying phenomenon is that much of the documented state surveillance in Africa targets key democracy actors. This practice extends to other jurisdictions beyond Africa where democracy deficits and outright authoritarianism are evident. As shown by United Nations experts[21] and Amnesty International,[22] surveillance is increasingly being used to spy on activists, journalists, opposition figures, and dissidents.

16 *Institute of Development Studies, Surveillance Law in Africa: a review of six countries, 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y*

17 *Bulelani Jili, The Spread of Surveillance Technology in Africa Stirs Security Concerns, December 11, 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/*

18 *Oarabile Mudongo, Africa's Expansion of AI Surveillance — Regional Gaps and Key Trends, https://researchictafrica.net/publication/africas-expansion-of-ai-surveillance-regional-gaps-and-key-trends/*

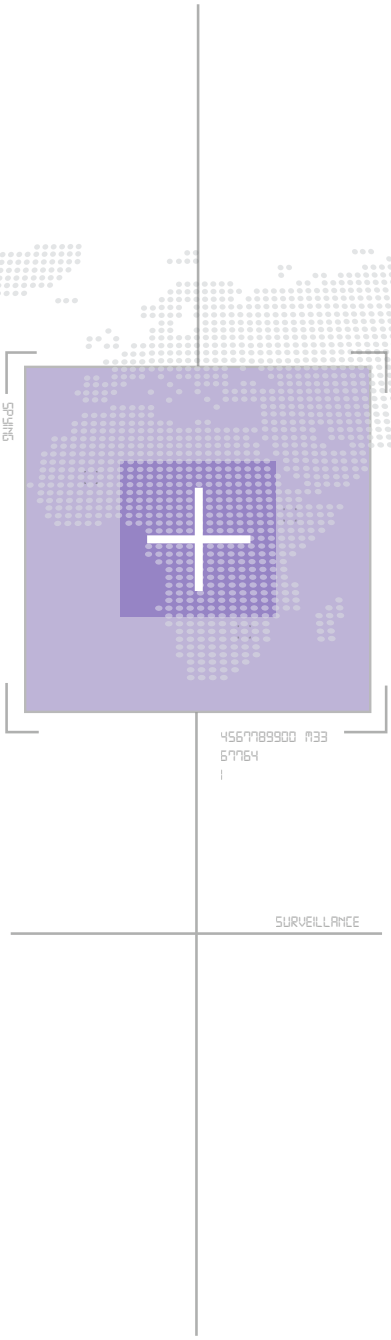
19 *How African Governments Undermine the Use of Encryption, https://cipesa.org/wp-content/files/briefs/How-African-Governments-Undermine-the-Use-of-Encryption-Oct-26.pdf*

20 *Mapping and Analysis of Privacy Laws in Africa, https://cipesa.org/wp-content/files/briefs/Mapping-and-Analysis-of-Privacy-Laws-in-Africa-2021.pdf*

21 *Report on the adverse effect of the surveillance industry on freedom of expression, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReportToHRC.aspx*

22 *When is targeted surveillance wrong? https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/*

Surveillance and Compelled Service Provider Assistance in Africa



In many African countries, the right to privacy is derogable, meaning national security, public order, and the investigation and detection of crime may be relied upon as valid justifications to limit the right. Such limitations are recognised in national constitutions and could also be important for protecting fundamental rights and freedoms. However, governments need to ensure that the limits are lawful, necessary, proportionate and justifiable in a free and democratic society. Moreover, states should put in place oversight mechanisms and sufficient checks and balances to prevent the abuse of surveillance power or exploitation of loopholes in existing laws.

The expansion in state surveillance is a key component of a wider arsenal of controls designed and deployed by several African governments to undermine digital rights and clamp down on their citizens' ability to openly and freely use digital technologies. Such measures curtail the right to free expression, access to information, peaceful assembly and association that are central to citizen participation in democratic processes.

Indeed, studies in various countries have found that surveillance practices cause HRDs to self-censor and refrain from exercising their rights due to easy identification and ease of traceability,[23] monitoring and tracking which undermine encryption and confidentiality and are often accompanied by arrests, threats and intimidation.[24]

> The failure to enact comprehensive privacy laws, in the absence of effective constitutional guarantees to the right, opens the door for unchecked executive surveillance powers, and leaves citizens with weak due process safeguards, and limited opportunities to exercise or enjoy their rights, and seek redress in cases of abuse … The place of independent judicial oversight over surveillance operations remains problematic in various countries. In some countries, surveillance operations are entirely carried out and overseen by bodies within the executive. - *Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa*

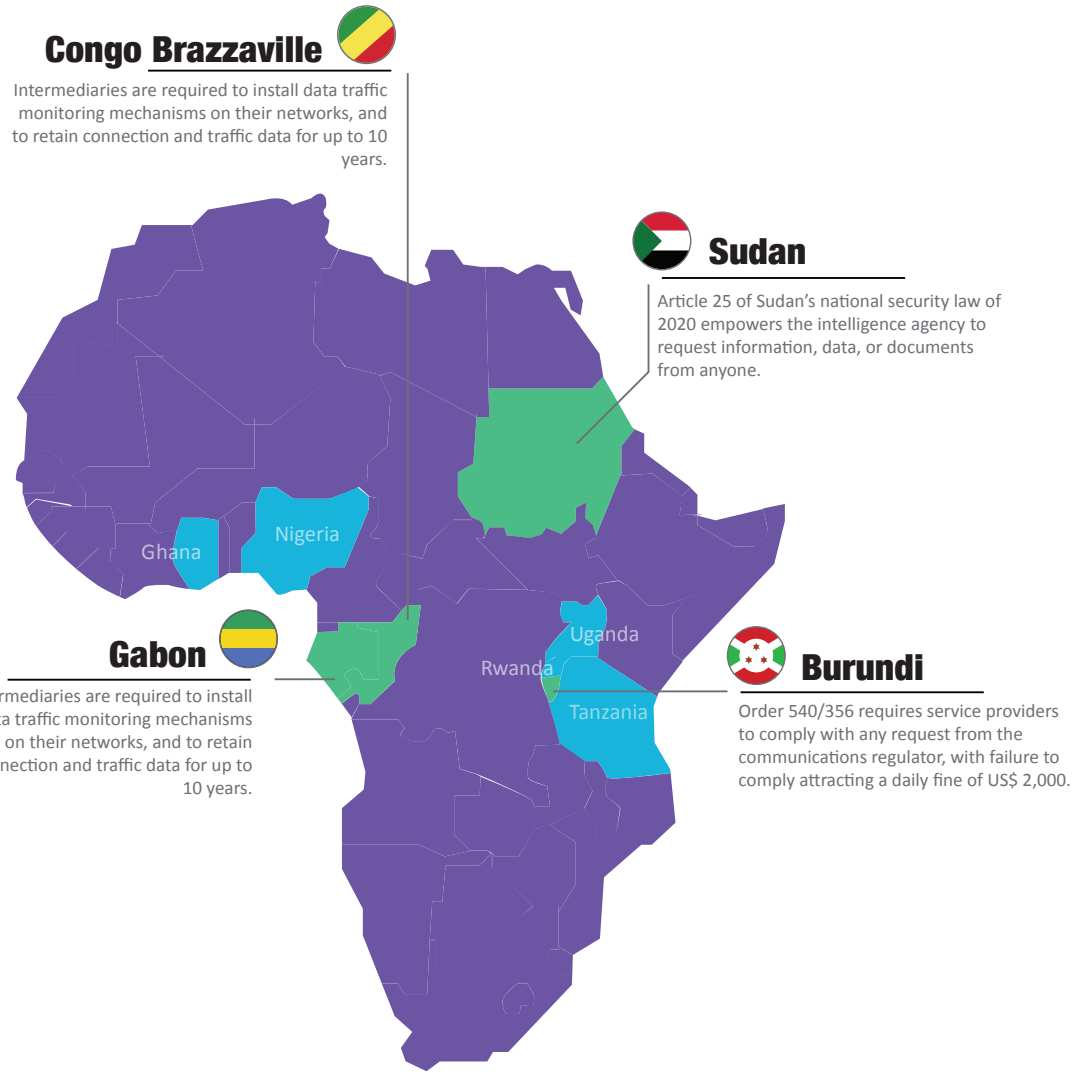
In their bid to entrench surveillance, various countries have introduced provisions requiring mandatory compliance by third parties to government interception requests. Laws in Cameroon, Rwanda, Uganda, Zambia, and Zimbabwe require intermediaries such as telecom companies and ISPs to install equipment and software on their networks that provide back doors to enable state agencies to intercept communications, including in real-time, for such periods as may be required. Similarly, articles 38 and 40 of Sierra Leone's Cybersecurity and Cybercrime Act 2021 require electronic communication service providers to ensure that they use a system that is technically capable of supporting lawful interceptions. The penalties for non-compliance with these requirements across the various countries are often punitive.[25]

23 ISOC, Intermediaries and Encryption, https://www.internetsociety.org/resources/doc/2020/fact-sheet-intermediaries-and-encryption/

24 Amnesty

25 Imperilled

For example, article 10 of Burundi's Order 540/356 requires service providers to comply with any request from the communications regulator, with failure to comply attracting a daily fine of US$ 2,000.[26] In Congo Brazzaville[27] and Gabon,[28] intermediaries are required to install data traffic monitoring mechanisms on their networks, and to retain connection and traffic data for up to 10 years. Meanwhile in Sudan, telecom operators are obliged to permit the telecoms regulator to enter their sites, network and equipment and install the necessary devices to measure and monitor their performance.[29] Article 25 of Sudan's national security law of 2020 empowers the intelligence agency to request information, data, or documents from anyone. Notably, legal loopholes such as in the laws of Uganda, Rwanda, Nigeria, Ghana, and Tanzania, where surveillance can be conducted without obtaining a court order or on the basis of an oral application for interception, remain of concern.[30]



26 Article 9 Order No 540/356 of 17 March 2016, http://arct.gov.bi/images/ordonnances/ordo540356 .pdf, allows the telecoms regulator to request the full identity of an internet subscriber and their IP address, and install IP probes on the technical installations of an ISP.

27 Article 21 of the Cybersecurity Act of 2020

28 Article 12 of the Order on Cyber Security and the Fight against Cybercrime of February 2018.

29 Article 25 of the 2018 Telecommunications and Postal Regulation Act

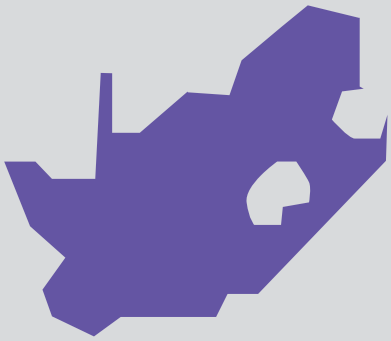
30 CIPESA, State of Internet Freedom in Africa 2021, https://cipesa.org/?wpfb_dl=467

These requirements contravene Principle 11 of the "Necessary and Proportionate" guidelines, which provides that states should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for state communications surveillance purposes.

Another common element in the laws of several countries are legal requirements which undermine encryption. For example, encryption service providers may be required by law to assist on request or on the orders of state agencies, including judicial authorities, law enforcement agencies and regulators, to not only hand over the encrypted data in their custody, but to decrypt such data before handing it over to state authorities.[31] Such requirements are evident in article 635 of Benin's Digital Code and article 78 of its Code of Criminal Procedure, article 52 of Niger's 2017 data protection law, article 16 of Cote d'Ivoire's Decree No. 2014-105, article 34 and 37 of Gabon's law on cyber security and the fight against cybercrime, articles 19 and 36 of Chad's Law no 009/PR/2015 on Cybersecurity and Cybercrime and, Sierra Leone's cybercrimes law of 2021.

Other noteworthy practices that undermine encryption include legal requirements for the registration and licensing of encryption service providers and the extensive powers granted to regulators to prohibit the use of some encryption technologies. These measures make it easy for regulators and other government agencies to access information held by encryption services providers, including decryption keys and encrypted data. Ultimately, they undermine best practices which require governments to refrain from adopting laws, policies, and practices that limit access to or undermine encryption and other secure communications tools and technologies.[32]

Lessons from South Africa



South Africa stands out in the region for having a law that requires strong oversight over state surveillance. The country's Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) requires a judge's assessment to allow for surveillance.[33] But even with its robust law, the Constitutional Court found that sections of RICA violated the Constitution, in a case brought by journalist Sam Sole of AmaBhungane, who was being spied on by the state without his knowledge.[34] [35] [36] Furthermore, a 2018 report by Right to Know on surveillance of journalists in South Africa detailed 12 cases of surveillance, interception of communications and illegal accessing of call records by private investigators and the state. These were conducted through the criminal intelligence system, which carried out surveillance on journalists that were working on various cases, including those on public corruption.[37] Moreover, in March 2021, an investigative journalist was reported to be under illegal surveillance and his communication was allegedly intercepted by the police's crime intelligence in their attempt to determine his sources behind the coverage of issues within police management.[38]

31 How African Governments Undermine the Use of Encryption, https://cipesa.org/?wpfb_dl=477

32 See The Letter here: https://securetheinternet.org/#letter

33 The Surveillance State: Communications surveillance and privacy in South Africa, https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillan-Cestate-web.pdf

34 amaBhungane's Rica victory: Big Brother can no longer watch us with impunity, https://www.dailymaverick.co.za/article/2021-02-07-amabhunganes-rica-victory-big-brother-can-no-longer-watch-us-with-impunity/

35 Sanef condemns alleged illegal surveillance of News24 journalist by Crime Intelligence, https://www.news24.com/news24/southafrica/news/sanef-condemns-alleged-illegal-surveillance-of-news24-journalist-by-crime-intelligence-20210308

36 https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf

37 https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf

38 Sanef condemns alleged illegal surveillance of News24 journalist by Crime Intelligence, https://www.news24.com/news24/southafrica/news/sanef-condemns-alleged-illegal-surveillance-of-news24-journalist-by-crime-intelligence-20210308

Individuals' Call Data Requests

One of the ways in which intermediaries, notably telecom companies and ISPs, are compelled to support governments' monitoring of citizens' communications is by offering either call data or monitoring assistance. It is disconcerting that many telecom companies operating in Africa do not issue any or detailed transparency reports to show how they handle government requests for users' data. The excuse given by some companies is that the laws in particular countries do not allow them to make such information public, or that the internal human rights policies of the companies are not yet matured enough to enable them to publish such information.

Over the past few years there have been increased requests for call data by government and security agencies.[39] In 2014, Vodafone revealed that governments in some of the 29 countries where it had operations, including the Democratic Republic of Congo (DR Congo), South Africa, Lesotho, Tanzania, Mozambique, Kenya, Egypt and Ghana had made several requests for subscribers' data, sometimes without warrants.[40] The operator noted that it had received around 100,000 requests from African governments for metadata such as phone numbers, addresses, device locations and times of calls and text messages, with the governments making most requests including Tanzania (98,765 requests), DR Congo (436) and Lesotho (488).

In 2020, Vodafone received 1,249 requests from the government of the DR Congo.[41] In the same year, according to the Vodafone Transparency Report, Lesotho made 2,478 requests while Tanzania made 15,338 requests. The MTN Group Transparency Report for the financial year 2021 also indicates that several countries ask the operator for users' call data. During the year, MTN received up to 110,140 data requests related to criminal investigations, 47,534 requests for subscribers' location disclosure, and 55,275 requests to suspend or deactivate subscribers' SIM cards.

39 *https://cipesa.org/wp-content/uploads/2017/08/Screen-Shot-2017-08-23-at-15.57.16.png*

40 *Ashnah Kalemera & Juliet N. Nanfuka, Vodafone Reveals Government Requests for Subscriber Information, https://cipesa.org/2014/07/vodafone-reveals-government-requests-for-subscriber-information/*

41 *Vodafone, Country by Country Disclosure of Law Enforcement Assistance Demands 2019-20, https://www.vodafone.com/sites/default/files/2021-02/Vodafone_LED_country_by_country_2019-20_AW4_V4.pdf*

Failure to Adhere to International Standards

Where the conduct of state surveillance is inevitable, it should be carried out based on the acceptable regional and international human rights standards and business best practices. Guidance on the standards to adhere to on the conduct of communication surveillance are elaborated under the Declaration of Principles on Freedom of Expression and Access to Information in Africa developed in 2019[42] by The African Commission on Human and Peoples' Rights (ACHPR); and the International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), which were developed in 2013 in a global effort by numerous human rights organisations.[43]

Principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa

Privacy and communication surveillance

1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.

2. States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.

3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:
    a. the prior authorisation of an independent and impartial judicial authority;
    b. due process safeguards;
    c. specific limitation on the time, manner, place and scope of the surveillance;
    d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
    e. proactive transparency on the nature and scope of its use; and
    f. effective monitoring and regular review by an independent oversight mechanism.

The International Principles on the Application of Human Rights to Communications Surveillance [44]

The principles, which were developed in 2013 by an international coalition led by the Electronic Frontier Foundation and signed by more than 600 entities, clarify how international human rights law applies to communications surveillance. Below is a summary of the principles.

42 Declaration of Principles on Freedom of Expression and Access to Information in Africa developed in 2019 https://ihrda.uwazi.io/api/files/1605623598849dpiuruykv5p.pdf

43 Necessary and Proportionate, https://necessaryandproportionate.org/

44 The International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/principles/

Principle	Explanation
1. **Legality**	Any limitation to human rights must be prescribed by law
2. **Legitimate aim**	Laws should only permit communications surveillance to achieve a legitimate aim that corresponds to an important legal interest that is necessary in a democratic society.
3. **Necessity**	Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim.
4. **Adequacy**	Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific legitimate aim identified.
5. **Proportionality**	Communication surveillance must be regarded as a highly intrusive act that interferes with human rights and threatening the foundations of a democratic society. Decisions about communications surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.
6. **Competent judicial authority**	Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.
7. **Due process**	States shall respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.
8. **User notification**	Those whose communications are being surveilled should be notified of a decision authorising communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies.
9. **Transparency**	States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities.
10. **Public oversight**	States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.
11. **Integrity of communications and systems**	States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for state Communications Surveillance purposes.
12. **Safeguards for international cooperation**	In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States.
Safeguards against illegitimate access and right to effective remedy	States should enact legislation criminalising illegal Communications Surveillance by public or private actors.

The surveillance practice in many African countries profoundly fails to adhere to these ACHPR Principles and to the Necessary and Proportionate guidelines. This is evident in their failure to comply with principles such as due process, judicial oversight, public oversight, and transparency. The practices also fall short on Principle 11 on the integrity of communications and systems. According to Principle 11, restricting states from compelling services providers to facilitate communication surveillance is necessary in order to ensure the integrity, security and privacy of communication systems, which when interfered with also compromises security generally. It adds: "A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users."

The United Nations Guiding Principles on Business and Human Rights (UNGPs)

The failure to adhere to the ACHPR principles as intermediaries labour to comply with national laws and licensing obligations, often results in failure to fulfill the UNGPs, which require companies to prevent human rights abuses in their operations and provide remedies if such abuses take place.

The UNGPs provide, for example in principle 11 and principle 13, that businesses must seek to prevent or mitigate any adverse impacts related to their operations, products or services, even if these impacts have been carried out by suppliers or business partners.[45]

Meanwhile, Principle 23 provides that, in all contexts, business enterprises should comply with all applicable laws and respect internationally recognised human rights, wherever they operate; seek ways to honour the principles of internationally recognised human rights when faced with conflicting requirements; and treat the risk of causing or contributing to gross human rights abuses as a legal compliance issue wherever they operate.

Key to telecom operators' compliance with the UNGPs is the development and implementation of strong human rights policies, which spell out how government requests for users' data and for surveillance interception are assessed before compliance or rejection. An instructive case here is of MTN. By its recently developed human rights policy, MTN committed to protecting its customers' privacy, keeping information safe and ensuring the security of personal information. Further, MTN committed to stand by the UNGPs, which, it noted, "encourages sound governance and supports the lawful assessment of government directives." Per its Transparency Report for 2021, in August 2021, MTN South Sudan "successfully lived by this principle and protected the privacy and safety of our customers by implementing MTN's digital human rights policy and due diligence approach when it received a directive for customer data." This assessment and decision to not disclose data was guided by written policy measures and stated commitment to stand by the UNGPs.

45 OHCHR, The UN Guiding Principles on Business and Human Rights: An Introduction, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

Conclusion and Recommendations

The brief shows that compelling service provider assistance is one of the main avenues African governments are using to aid their communication surveillance practices. Common across various countries are flawed laws that are embedded with broad and ambiguous provisions, which are often implemented in an opaque environment where impunity and abuse by state security agencies reigns supreme.[46]

A further concern is the lack of comprehensive checks and balances including independent oversight by judiciaries, parliaments and data protection bodies of the communication surveillance practices by state agencies within executive arms of government. Moreover, national programmes such as mandatory SIM card registration, public CCTV cameras and the creation of inter-linked national biometric digital identity databases could enable surveillance especially where scope creep is not checked.

Overall, the net effect of the communication surveillance is its tremendous impact on the ability of citizens to meaningfully participate in democratic processes. In essence, the practice limits individuals' ability to enjoy their rights to privacy, access to information, and freedoms of expression, assembly and association. These rights are intricately linked and are critical in facilitating citizens' participation in public affairs. Therefore, enforcement of flawed laws and policies that facilitate communication surveillance, in the absence of strong legal safeguards coupled with weak oversight, often constricts civic space as it creates fear and apprehension among citizens and vitiates their ability to freely and meaningfully engage in democratic processes.

Recommendations

In order to defend, restore and promote human rights that are undermined by state surveillance, we recommend the following:

Governments

- Develop, review, update and strengthen national laws, policies and practices on state surveillance in order to bring them into compliance with well-established international human rights standards including as elaborated in Principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, and the International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles).
- Ensure that surveillance, privacy and data protection laws, standards and guidelines are developed taking into consideration views and input of all relevant stakeholders.
- Revise national laws governing state surveillance to ensure that they provide for clear and robust oversight over surveillance including by judicial and legislative bodies.
- Implement the actionable steps and meet their obligations with respect to the protection of the right to privacy under the protect, respect and remedy framework in the UN Guiding Principles on Business and Human Rights, including moving towards mandatory human rights due diligence, which could be instrumental in regulation of technologies and the tech sector.
- Refrain from compelling service providers and intermediaries to facilitate communication surveillance including through data requests on the identity and activities of users, weakening encryption, limiting anonymity, creation of backdoors, requiring logging of user activity or compromising privacy of users, in the absence of lawful warrants or court orders that are necessary and proportionate in the circumstances and adequate judicial oversight.

46 https://cipesa.org/2021/09/how-state-surveillance-is-stifling-democratic-participation-in-africa-state-of-internet-freedom-in-africa-study-findings/

Technology Companies

- Speak out on national laws, policies and directives that place undue obligations and liability on intermediaries and hinder them from fulfilling the UNGPs.
- Monitor their performance and promote transparency and accountability by regularly publishing privacy policies and transparency reports and inform users about the collection, use, handling, sharing and retention of their data that may affect their right to privacy.
- Conduct human rights due diligence to identify, prevent or mitigate risks of compelled service provider assistance and surveillance on the lifecycle of the products and services and their business operations.
- Develop rights-respecting policies, responsible business practices and culture in line with international human rights standards such as the UNGPs and the Necessary and Proportionate principles, with a key aspect of such policies focusing on how the companies assess government requests for users' data and for surveillance support.

Civil society

- Adopt a multi-stakeholder approach to digital rights advocacy as a critical avenue to promote shared understanding of the human rights risks and impacts of technology and communication surveillance in Africa.
- Collaborate with other stakeholders in various African countries to advocate against continued unchecked communication surveillance and to promote the adoption of international human rights standards on privacy and data protection.
- Conduct strategic public interest litigation to challenge laws, policies, practices and directives that threaten the right to privacy, such as those on compelled service provider assistance, and obtain remedies for victims of illegal state surveillance

Academia

- Conduct research to promote greater understanding of the human rights risks on communication surveillance and the technology business models on the continent.
- Review the surveillance, privacy and data protection laws, standards and guidelines and propose domestically-driven policy solutions on how to entrench and domesticate international human rights standards and principles on the right to privacy.
- Facilitate multi-stakeholder engagement to enable shared understanding of appropriate regulatory approaches to confront common concerns and illegitimate uses of technology for communication surveillance.

Media

- Conduct investigative journalism and expose communication surveillance practices of African governments so as to ensure accountability by the perpetrators of illegal and unwarranted surveillance.
- Build the capacity of journalists in the use of digital security tools to enable them to detect, prevent and circumvent communication surveillance that targets them.
- Build the capacity of journalists on the various international human rights standards on privacy and communication surveillance.
- Partner with civil society actors including academia to document, report and improve coverage of advocacy and research about communication surveillance.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Tel: +256 414 289 502
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org