State of Internet Freedom in Africa 2021

Effects of State Surveillance on Democratic Participation in Africa

September 2021
# Table of Contents

1.0 Introduction 3  
2.0 Methodology 6  
3.0 Surveillance Laws in Africa 7  
  3.1 Imposition of Liability on Intermediaries 7  
  3.2 Excessive Powers Amidst Weak Oversight 8  
  3.3 Enhanced Capacity to Intercept Communication and Conduct Surveillance 10  
  3.4 Procurement and Installation of Surveillance Technology 10  
  3.5 Biometric Data Collection, including SIM Card Registration 12  
4.0 Results 15  
  4.1 Manifestations of and Experiences with Surveillance 15  
    4.1.1 Physical Surveillance 15  
    4.1.2 Interception of Communications 17  
    4.1.3 CCTV Surveillance 18  
  4.2 Effects of Surveillance on Civic Engagement and Democratic Participation 19  
    4.2.1 Undermining the Right to Freedom of Expression and Access to Information 19  
    4.2.2 Infringing on the Right to Privacy of Communications 21  
    4.2.3 Curtailing Freedom of Assembly and Association 22  
    4.2.4 Curtailing Freedom of Movement 23  
    4.2.5 Effect on the Work of Organisations 24  
    4.2.6 Impact on Personal Life and Relations 24  
    4.2.7 Effect on Psychological Well-Being 25  
  4.3 Mitigation Measures adopted to Cope with Surveillance 27  
  4.4 Discussion of Study Findings 28  
5.0 Conclusions and Recommendations 30  
  5.1 Conclusions 30  
  5.2 Recommendations 30
Africa has increasingly become digitalised with technology playing a pivotal role in learning, working, and public participation. However, there is growing concern that rising state surveillance is not only undermining African citizens’ digital rights, but also hindering their willingness to meaningfully embrace these transformative technologies. State surveillance generally refers to measures taken by governments aimed at monitoring and supervising activities of the population. Surveillance involves the monitoring, interception, collection, preservation, and retention of information that has been communicated, relayed, or generated over communication networks to a group of recipients by a third party.

In the past few years, increasing state surveillance in Africa has become a key concern. Many countries across the continent have enacted various 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, require the localisation of personal data, and grant law enforcement agents broad search and seizure powers.

In countries such as Chad, Malawi, Senegal, Tanzania, Tunisia and Zambia, laws prohibit offering encryption services without licensing, and in other cases, encryption service providers are required to decrypt any encrypted information that they hold so as to aid lawful interception. Similarly, while all countries have laws that facilitate lawful surveillance, many of these laws have pervasive flaws, are partially implemented, indiscriminately applied, and widely abused.

While state surveillance is justifiable to promote national security, it is increasingly being used by various African governments to entrench political control, including through targeted profiling and spying on activists, human rights defenders, journalists, opposition leaders, and political dissidents perceived to be critical of the ruling administrations. A 2019 United Nations experts report warned that surveillance of individuals – often journalists, activists, opposition figures, and critics – had thrived amid weak controls on exports and transfers of technology to repressive governments.

The continued rise in surveillance cannot be divorced from the growing affronts to digital civic space in the region. State surveillance is a key component of wider efforts by a significant number of African governments deployed in an ever-expanding raft of measures to undermine and clamp down on their citizens’ ability to openly and freely use digital technologies. Such control measures are specifically aimed at curtailing expression and organising that is critical of governments and state officials. These controls are heightened in instances where the ruling parties’ hold on power is threatened such as in times of political contestation, including during protests, political rallies, election, referenda, political debates on constitutional change, governance, corruption and accountability.
Indeed, autocratic governments have complemented their surveillance practices with attacks on digital rights to further stifle opposition or criticism. Several countries in Africa have carried out internet shutdowns and disruptions to stop the flow of information on the internet. Moreover, some governments conduct misinformation and disinformation campaigns on the one hand, but on the other, introduce “false news” laws which are deployed by state security agencies to silence, intimidate, harass, detain, and prosecute government critics and thus perpetuate state narratives on any given issue.

Further, some states have invested in building the technical capacity of their security agencies who are permitted to exploit surveillance, cybercrime and terrorism laws and carry out widespread surveillance and interception of communication, often with limited judicial oversight or accountability. This has, for example, entailed the acquisition of software and equipment with capacity to conduct digital surveillance, enforcing mandatory Subscriber Identification Module (SIM) registration laws that requires all communications users to link their electronic communications to their legal identities for the purpose of fighting cybercrime, and ordering telecommunication service providers to acquire systems that have backdoors to enable monitoring and interception of private communication without adequate checks and balances.

The lack of transparency in the purchase and use of surveillance technologies, the growing states’ capability for mass surveillance and their targeting of non-state actors critical of governments are a cause for concern. Closed Circuit television camera (CCTV) surveillance technology, especially those with facial recognition capability and Spyware that enables "remote control hacking" and eavesdropping are some of the measures gaining traction in Africa. For instance, Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria, Zambia and Zimbabwe are among the countries named as likely to be using Circles’ surveillance platforms to exploit flaws in telecoms systems to access telephone calls, SMS messages and location services, which were supplied by the firm affiliated with the Israel-based NSO Group. Similarly, Morocco, Rwanda and Togo are among governments identified as using the Pegasus spying software. Also, employees of Huawei, which has supplied video surveillance technology to many states, reportedly helped African governments to spy on their political opponents, including by intercepting their encrypted communications and social media, and using cell data to track their whereabouts.

Surveillance undermines the privacy of communications and the right to anonymity, and consequently leads to self-censorship and the withdrawal of some individuals and groups from the online public sphere. Moreover, surveillance systems, both targeted and mass, “may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.”

Moreover, while protections against arbitrary or unlawful surveillance have focused on guaranteeing the right to privacy, these interferences also erode and have a chilling effect on the rights to freedom of expression and opinion, access to information, assembly and association and to political participation.\textsuperscript{12} Indeed, studies have shown that the use of surveillance technologies and people’s awareness of being watched and tracked “might lead to people’s refusal to join public assemblies, participating in social and cultural life, and feeling constrained to freely express their thoughts, conscience and religious beliefs in public spaces.”\textsuperscript{13} The importance of these rights in the digital age reinforces the need for sufficient protections to safeguard their enjoyment.

This research discusses the nature and adverse effects of state surveillance on human rights defenders (HRDs), civil society organisations, activists, journalists, and political opposition leaders and groups in 11 African countries - Cameroon, Ethiopia, Kenya, Mozambique, Nigeria, Rwanda, Tanzania, Tunisia, Uganda, Zambia, and Zimbabwe. It maps the prevalent forms of surveillance, the laws and policies that aid surveillance, and the impact of state surveillance on


Methodology

The study was conducted through a combination of desk research, policy analysis, and key informant interviews. Desk research and policy analysis were employed to examine the laws and policies that enable state surveillance and interception of communication in the countries under study. Besides setting out the regulatory landscape and associated controversies, the desk research and policy analysis provided a contextual analysis of how surveillance potentially casts a chilling effect on rights and freedoms.

Furthermore, the research conducted a total of 57 key informant interviews with individuals who have experienced state-sponsored surveillance as well as staff of non-government entities that closely work with those who have been victims of state surveillance from the study countries. The respondents were drawn from Cameroon, Ethiopia, Kenya, Mozambique, Nigeria, Rwanda, Tanzania, Tunisia, Uganda, Zambia and Zimbabwe. The respondents included members of civil society, journalists as well as government critics, political party representatives, lawyers, academics, and bloggers. Of the 57 respondents interviewed, 32% were female, 65% were male, while the rest preferred not to indicate their gender.

These interviews captured first-hand experiences of victims of state surveillance. The research took a particular interest in collating individuals’ experiences and giving voice to those who had experienced surveillance. The report draws on the narratives of these individuals to illuminate the implications of surveillance on political and democratic participation in Africa.
Surveillance activities in Africa, including the interception of digital communications, collection of personal data including biometric data, video surveillance and the use of facial recognition technology, as well as physical search and seizure, are enabled by several laws and regulations. The fact of having this legislation may not be a major concern in itself, as governments all over the world have a legitimate interest in conducting lawful surveillance. The concerns in the region are the broad powers given to the state and its agencies to conduct surveillance, the abuse of the surveillance powers, and the limited oversight and transparency over surveillance activity. Additional concerns include the strenuous and sometimes unclear demands on intermediaries, including to facilitate interception of communication or hand over communication data of their subscribers to state security agencies. In this subsection, we look at the relevant laws and some of their contentious provisions.

3.1 Imposition of Liability on Intermediaries

Many countries, including Cameroon, Rwanda, Uganda, Zambia, and Zimbabwe require intermediaries such as telecom companies and Internet Service Providers (ISPs) to facilitate surveillance including by installing equipment and software that enable governments to lawfully intercept communications on their networks, including in real-time for such periods as may be required.

The effecting provisions mirror each other across the continent. They include article 25 of Cameroon’s Law n°2010/012 of 21 December 2010 on Cybersecurity and Cybercrime; article 61 of Chad’s Cybersecurity and Cybercrime Act; section 53 of Kenya’s Computer Misuse and Cybercrimes Act, 2018; article 7 of Rwanda’s Interception of Communications, 2013; article 11(3-4) of Tunisia’s Decree No. 4773 of 2014 regulating the operations of ISPs;14 section 11 of Uganda’s Regulation of Interception of Communications Act, 2010, section 38 of Zambia’s Cyber Security and Cyber Crimes Act, and section 12 of Zimbabwe’s Interception of Communications Act, 2007.15

The penalties for non-compliance with these requirements are often punitive. In Uganda, failure to comply with the requirement to support interception attracts a fine of UGX 2 million (USD 583) or imprisonment for a period not exceeding five years, or both. In Zambia the penalty is a fine of 150,000 Kwacha (USD 6,643), imprisonment for up to five years, or both. Such a high penalty as stipulated in Zambian legislation will compel service providers to render interception assistance even when they receive dubious oral orders that lack judicial backing or any evidence justifying the interception. In Kenya, the penalty for not complying with a interception order from the court is a fine of 10 million shillings (USD 90,530) where the service provider is a corporation, and in case of an officer of the service provider, a fine of up to 5 million shillings (USD 45,265) or imprisonment for up to three years, or to both.

Yet there are other onerous demands that are placed on the shoulders of intermediaries. In Chad, article 51 of the 2020 Cybersecurity and Cybercrime law requires service providers to keep all data that enables the identification of any person who contributed to content creation in services they provide for a period of 10 years. The same requirement is found in Cameroonian law. In Ethiopia, article 23 of the Computer Crime Proclamation No. 958/2016 (2016) requires service providers to retain all computer data disseminated through their computer systems or data relating to data processing or communication service for at least one year and they must disclose this data on the order of a court or a public prosecutor.

Meanwhile, some countries, notably Tanzania, place burdensome requirements on internet cafes. Regulations 13(1)(d) of the Electronic and Postal Communications (Online Content) Regulations, 2020 obligates Internet Café service providers to install surveillance cameras inside cafes to monitor users’ activities. The same provision requires registration of all customers of internet cafes, who are required to produce a national ID card. Nigeria has also made moves in this direction, with the Nigerian Communications Commission in 2013 directing all cyber café operators to register and maintain a database of their users’ full names, physical addresses, telephone numbers, and to take their passport photos.

3.2 Excessive Powers Amidst Weak Oversight

Laws in various countries have criminalised illegal surveillance and also place various safeguards on the conduct of state surveillance by requiring a judicial authority to authorise surveillance. The laws in Kenya, Nigeria, Tanzania, Tunisia, Uganda, for example, require an interception warrant or order from a judicial officer in order to conduct monitoring and interception of communications. Nonetheless, the broad powers handed to state agencies, limited oversight over and accountability for communications interceptions, and provisions that allow for interception without a warrant present cause for concern. Moreover, some of the laws provide a wide and vague array of undefined grounds on which interception of communications can be conducted.

In Zimbabwe, the interception law does not provide for judicial oversight in issuance of warrants; instead, it grants the powers to the minister in charge of communications or any other minister assigned by the president to issue such interception orders. Equally worrisome is the scenario in other countries like Rwanda, Uganda, and Zambia, where a warrant for interception can be made orally, and in other countries such as Nigeria and Tanzania, where interception can occur without a warrant from any authority.

In Ethiopia, the Computer Crime Proclamation No. 958/2016 (2016) provides for both a warrant to be issued by court following an application by an investigatory organ, and authority to the Attorney General to give permission to the investigatory organ to conduct interception or surveillance without a court warrant “where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed” (section 25). In the latter case, the Attorney General shall present the reasons for interception or surveillance without a court warrant to the President of the Federal High Court within 48 hours, “and the president shall give appropriate order immediately.”
In Nigeria, Sections 4 and 7 of the Lawful Interception of Communications Regulations 2019\(^\text{22}\) give powers to government agencies such as the Office of the National Security Adviser (represented by the National Security Adviser or his designee) or the State Security Services (represented by the Director or his designee),\(^\text{23}\) to intercept communications without a warrant, through communications licensees. Section 8 of the Nigerian regulations provides additional conditions where interception of communications can be carried out without a warrant. In addition, section 38 of the Nigeria Cybercrime Act 2015 empowers law enforcement officials to have access to data from service providers without obtaining a warrant.\(^\text{24}\) Specifically, section 38(3) notes that, a law enforcement agency may, through its authorised officer, request for the release of any information and it shall be the duty of the service provider to comply.

In many countries, security agencies possess broad search and seizure powers, which are open to misuse given the low oversight and accountability over interception activities. In Chad, under article 27 of the Cybersecurity and Cybercrime Act, judicial police officers and authorised agents of the National Agency for Computer Security and eCertification (ANSICE) may use the appropriate technical means to collect or record in real time, data relating to the content of electronic communications. The law further prescribes the use of a software remotely installed on a computer system to collect evidence (article 31). Section 54 of the Criminal Procedure and Evidence Act of Zimbabwe similarly provides 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.

In Tanzania, Section 31 of the Tanzania Cybercrimes Act, 2015 gives powers to the police officer in charge of a station to search and seize or authorise the search and seizure of communication devices or data in conducting investigations. Section 31(1) gives such powers to a police officer in charge of a police station or a law enforcement officer of a similar rank, to (enter into any premise and search or seize a device or computer system; secure the computer data accessed; or extend the search or similar accessing to another system where a law enforcement officer conducting a search has grounds to believe that the data sought is stored in another computer system or part of it.

In Uganda, the Anti-Terrorism Act Part VII (sections 18 to 22) provides for the interception of communications and surveillance on grounds such as the public interest, national economy and security, prevention of crime and protection of human rights and freedoms. Part VII of this law has been reinforced by section 2 of the Regulation of Interception of Communications Act which provides for control of interception. Further, the Computer Misuse Act (section 28) provides for searches and seizures, which potentially facilitates surveillance on the activities of individuals. Article 52(1) of Rwanda’s Law No. 44/2001 of 30/11/2001 Governing Telecommunications empowers the minister in charge of telecommunications policy and law, to “interrupt or cause to be interrupted, any private communication which appears dangerous to the national integrity, contrary to law, public order or public morals.”\(^\text{25}\)

Under sections 29 and 30 of Zambia’s Cyber Security and Cyber Crimes Act, 2021, an enforcement officer may intercept any communication and the request may be made orally to a service provider “on reasonable grounds to prevent possible or inflicted bodily harm, loss of life or threats to kill oneself, or damage to property or actual or possible cause of financial loss.”\(^\text{26}\) On the other hand, under the Electronic Communications and Transaction Act, 2009, while law enforcement officers are required to apply for an order to a judge or the Attorney General for permission to conduct interception, the authorities may conduct communication interceptions for any offence, regardless of seriousness.\(^\text{27}\)

In Mozambique, although Article 68 of the 2004 Telecommunications Law provides for the secrecy of a user’s communications, it stipulates grounds for exceptions, including in criminal investigations and in the interests of national

---


\(^{23}\) Regulation 12(1) of the Lawful Interception of Communications Regulations, 2019


\(^{26}\) Implications of Zambia’s Act 2021 on Digital Rights, https://cipesa.org/?wpfb_dl=447

\(^{27}\) Section 66 of the Electronic Communications and Transaction Act, 2009 of Zambia.
safety and the prevention of terrorism. In addition, network providers must cooperate with the authorities regarding the legal interception of communications under Decree No. 33/2001. In Tunisia, the Organic Act No. 26 of 2015 Relating to the Fight Against Terrorism and the Suppression of Money Laundering grants an Investigative Judge or the Prosecutor of the Republic the power to issue interception orders. In addition, the Technical Telecommunication Agency (ATT) can collect data from the servers of telecom operators and ISPs.

In Cameroon, articles 49 to 51 of the Law n°2010/012 of 21 December 2010 on Cybersecurity and Cybercrime grants Judicial Police Officers power to intercept, record, or transcribe any electronic communication. If the intermediaries have encoded or encrypted the data transmitted, they are required to decrypt the communications before giving them to the police. On the other hand, article 92 of the 2007 Code of Criminal Procedure prescribes the interception, recording or transcription of any correspondence sent by telecommunication in the event of a crime punishable by imprisonment of at least two years.

3.3 Enhanced Capacity to Intercept Communication and Conduct Surveillance

Over the last few years, many African governments have continued to enhance their technical capacity to intercept and monitor electronic communications. This has among others, entailed the installation of equipment including software or spyware that enables remote control hacking and eavesdropping, deployment of video surveillance systems, some of which have facial recognition capabilities, and requiring communication service providers to acquire relevant systems, at their own cost, with the capacity to intercept users’ private communications and accessed by state security agencies.

The countries have also embarked on creating massive databases with a multitude of personal data, including biometric data, which tend to be linked to National Identity cards, voters’ cards and SIM card registration details. These data collection exercises and inter-linked databases have improved the precision with which state authorities can identify individuals, which makes it easier to conduct communication surveillance and track targets movements.

3.4 Procurement and Installation of Surveillance Technology

The use of spyware appears to be rising, with a number of countries increasingly being outed by research as among those who have acquired technology that allows governments to snoop on private communications. For example, in 2020, several countries, including Botswana, Equatorial Guinea, Kenya, Nigeria, Zambia, and Zimbabwe, were reported to be using the surveillance platform Circles, to exploit flaws in telecoms systems and to access telephone calls, SMS messages and location services. According to the report, Circles, which is affiliated with the Israel-based NSO Group, has deployed its platforms across Africa, helping state security departments to snoop on communications of opposition politicians, journalists, and protestors.

The findings on Circles came on the heels of other research that indicated the use of spyware, including from the NSO Group, by Africa governments. In September 2018, the Citizen Lab, a Canadian internet freedom watchdog, reported that it had found infections of Pegasus, a surveillance software developed by NSO Group, in 45 countries including Algeria, Côte d’Ivoire, Egypt, Kenya, Morocco, Rwanda, South Africa, Uganda, and Zambia. Pegasus is frequently used by governments to surveil journalists, human rights defenders, and the opposition. A year later in October 2019, WhatsApp reported that a vulnerability in their application was exploited to target Rwandan dissents with Pegasus. WhatsApp identified at least 1,400 people targeted by the vulnerability, of which a “considerable amount” were

30 More African countries are relying on an Israeli surveillance tool to snoop on private citizens https://qz.com/africa/1940897/nigeria-kenya-use-israeli-surveillance-tool-to-listen-to-calls/
31 Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries,
Rwandan. Targets included a journalist and a member of the opposition who were both living in exile. More recently in July 2021, it was disclosed that Morocco, Rwanda and Togo were among the governments using Pegasus.

According to a lawsuit which WhatsApp brought against the NSO Group, the Pegasus malware was designed to be remotely installed to enable the remote access and control of information, including calls, messages, and location, on mobile devices using the Android, iOS, and BlackBerry operating systems. It added that the spyware was designed to intercept communications sent to and from a device, including communications over iMessage, Skype, Telegram, WeChat, Facebook Messenger, WhatsApp, and others.

Investments in communication systems monitoring apparatus, as well as CCTV systems, have also been a key component of the burgeoning surveillance states in the region. In 2011, the Ethiopian government established the Federal Police Commission with power to investigate crimes relating to information networks and computer systems and install CCTV cameras. The Ethiopian authorities are reported to have actively shopped in the European market for advanced surveillance technologies, acquiring tools to spy not only on individuals living in Ethiopia, but also on Ethiopians in the diaspora. The government purchased FinSpy, a surveillance system sold by a firm first headquartered in the UK and later in Germany, to allow remote access to computers infected with FinSpy software. Hacking Team, an Italian company that provides “eavesdropping software” that “hides itself inside target devices” enabled the Ethiopian government to intercept the communications of opposition leaders and journalists, including those in the diaspora.

In Uganda the government is reported to have, in 2012, enhanced its mass surveillance capacity through the use of spyware, intrusion malware, and intelligent network monitoring systems. In July 2018, the Uganda communications regulator, UCC was reported to have installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification.

In Kenya, the government, in 2014 awarded Safaricom, the largest mobile phone services provider, a tender to set up a communications and security surveillance system at a cost of 14.9 billion shillings ($14.9 million). The CCTV system installed outside public places and along key roads was procured from Huawei and provides a direct link all security agencies electronically to a central command centre. In January 2015, the Zimbabwean government is reported to have acquired various cyber-surveillance technologies from the Iranian government. The equipment is said to have been used to aid the government to ratchet up suppression and snooping on political opposition and other organisations it considered a national security threat.

In Chad, human rights defenders and journalists reported to have been presented with a report containing all their telephone conversations and their SMS messages after they were arrested. According to an Amnesty International report, private telecommunication companies in Chad confirmed wiretapping and call monitoring practices, stating that the authorities justify it for national security reasons.

In Tunisia under former President Ben Ali’s rule, political opponents were placed under physical and electronic surveillance. Emails of political dissidents were routinely hacked or intercepted in transit using deep-packet inspection (DPI) technology. The DPI infrastructure was provided to the Tunisian government by the American companies Blue Coat and

References:
32 “Inside the WhatsApp hack: how an Israeli technology was used to spy,” Financial Times, October 29, 2019, https://www.ft.com/content/d91279ee-f98c-11e9-98f4-4d6c2005029
41 Amnesty International; Chad: Between Recession and Repression: The Rising Cost of Dissent in Chad; September 2017, p. 36
In 2016, the government of Mozambique began the installation of CCTV surveillance in the cities of Maputo and Matola, purportedly for security purposes. The project was allegedly awarded without a public tender.\textsuperscript{46} Also in 2016, there were reports that the Mozambican government was intercepting and surveilling citizens’ online communications, with the support of a Chinese company - ZTE.\textsuperscript{47}

Besides acquiring spyware, installing video surveillance systems and undertaking mandatory data collection exercises, governments in the countries under study have also been known to ask intermediaries to disclose users’ data. Such demands for users’ data are regularly made to telephone companies, and international social media platforms such as Facebook, Google, and Twitter,\textsuperscript{48} in order to aid states’ surveillance activity. Other service providers, such as ISPs and online discussion forums also face these requests for assistance to state surveillance. For instance, in Tanzania, Jamii Forums Executive Director, Maxence Melo was charged under Section 22(1) of the Cyber Crimes Act, 2015 and on April 8, 2020 convicted to one year in prison or a fine of 3,000,000 Tshs (USD 1,297) for “obstruction of a police investigation”. The charges stemmed from Melo’s alleged refusal to disclose the identities of whistle-blowers on his Jamii Forums platform.\textsuperscript{49}

### 3.5 Biometric Data Collection, including SIM Card Registration

The collection, processing and sharing of personal data is a critical component in facilitating surveillance and the identification of surveillance targets. In several countries, the laws require the mandatory collection of a wide range of information for the registration of telecommunications subscribers and for digital identity programmes. Some governments are also collecting biometric data in registering SIM card owners, voters and those that apply for national IDs. This has greatly undermined the ability of citizens to communicate anonymously, given the amount of personal data that is collected, retained and shared through these exercises, without adequate oversight and respect for individuals’ privacy rights. Concerns about the misuse of such data are exacerbated by the lack of data protection laws, absence of independent data protection authorities, or poor enforcement of such laws where they exist, as well as the loopholes in the regulation of interception of communication laws.

In Cameroon, article 6 of the Decree No. 2015/3759 on the identification of subscribers requires telecom SIM card subscribers to provide their original national identity card, valid residence permit for foreigners or any other document which replaces it, their exact address including location map, and the international mobile equipment identity number (IMEI) of their device.

In Zambia, Section 39 of the Cyber Security and Cyber Crimes Act 2021 requires electronic communication service providers to collect personal data from individuals including names, residential addresses and identity numbers contained in identity cards before entering into a contract for provision of any service. Moreover, under subsection (1)(c), the service provider may collect any other information considered necessary. The service provider is further charged with keeping proper records and updating them frequently.
Similarly, the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 under rule 4 requires all mobile network providers to register all SIM card subscribers. In 2018, Kenya adopted the Statute Law (Miscellaneous Amendments) Act, 2018 which created the National Integrated Identity Management System (NIIMS) a digital ID system otherwise known as ‘Huduma Namba’ intended to be the single source of personal information, including biometric data of all Kenyans as well as foreign residents in Kenya. In Mozambique, the Regulation for the Registration and Activation of Mobile Subscriber Identification Modules Decree of 2015 requires all communications operators to register all SIM cards with data such as name and address of customers.

In Tanzania, SIM card registration has been ongoing since 2009, and currently, it is not possible to register a SIM card unless the biometric information collected is verified against the National Identification Authority (NIDA) database, which was itself created under the Registration and Identification of Persons Act. Increasingly, public institutions in Tanzania have moved to make the National ID or National Identification Number (NINs) the “primary/mandatory requirement for identification for service provision, including institutions like the Higher Education Loans Board, the Tax Revenue Authority, Business Registration, Licensing Authority and the Government Recruitment Agency.” Under section 84 of the Electronic and Postal Communications Act of 2010, network operators are required to submit details of all subscriber numbers and devices to a central register, held by the telecommunications authority, to be updated monthly.

The extensive information collected under SIM card registration by itself enables governments to identify and track a vast number of citizens with ease. Yet governments in the region have steadily moved to link such data to the national ID and voters’ registration databases, as well as to various other services provision. In Nigeria, section 27 of the National Identity Management Commission (NIMC) Act of 2007 makes digital identity registration mandatory before citizens can access several public services, yet the west African country does not have a substantive data protection law. This law requires that details of persons in the database shall be identified using unique and unambiguous features such as fingerprints and other biometric information.

For its part, Uganda has developed a Biometric Voter Verification System (BVVS) with fingerprints and images of all registered voters. These voters’ records (which in the 2016 elections related to more than 15.27 million individuals) were sourced from the National Security Information System, which is managed by the National Identification and Registration Authority (NIRA) and is the basis for issuing national IDs. The BVVS uses fingerprints to match voter details to confirm that the person is on the voters’ roll for a given polling station. The data in the BVVs includes the name, place and date of birth, location of the polling station and fingerprints of the voter. The BVVS was also used in the 2021 elections, effectively disenfranchising citizens who did not possess national IDs. Section 9(2) of Uganda’s Regulation of Interception of Communications Act (RICA) requires telecommunication service providers to ensure that subscribers register their SIM cards. The registration of SIM cards was made mandatory in Uganda in 2012.

Zimbabwe introduced compulsory SIM card registration in 2013 through the Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration), which also created a centralised subscriber database of all users that is managed by the communications industry regulator. Regulation 8(2)(c) of the Postal and Telecommunications (Subscriber Registration) Regulations, 2014 provides that, through this database, the regulator shall, among others, assist law enforcement agencies in safeguarding national security.
In Rwanda, article 4 of the 2017 Regulation Governing SIM card registrations requires any licensee operating in the country or by its agents to register all subscribers and SIM card holders. A SIM card can only be activated after the registration of the subscriber’s personal information, which include, full names, date of birth, Identity Card number, registered telephone number, and gender.

In Chad, through Order n° 001/PR/ 2016 of January 4, 2016, the President of the Republic of Chad created the National Agency for Secure Documents (ANATS), a statutory body under the supervision of the Minister in charge of security with the mandate to collect the biometric and biographical data necessary for identifying persons and producing secure documents. In the same year, the biometric system was extended to citizens of voting age in preparation for the 2016 presidential elections. It was argued that with a biometric voter card, each voter could be registered only once and this would make it possible to avoid the voters’ roll inflation experienced in previous elections.

Ethiopia’s 2012 Vital Events and Registration Proclamation requires the collection and storage of biometrics of citizens in a centralized system as part of efforts to provide citizens with national identity cards that contain identification numbers for citizens. However, the stored information could be disclosed to other organs for specified purposes such as national intelligence and security, crime prevention and investigation, tax collection, administrative and social services, implementation of financial risk management, and other purposes promulgated by law.

Amidst this expansive collection of data, some countries have legislated that personal data must be stored locally, with any cross-border data transfers to be authorised by data protection authorities. Such requirements are to be found in all the countries that have data protection laws, but for some countries they are found in laws regulating telecoms, finance and banking. Hosting data locally could grant state surveillance apparatus in some countries in the region easier access to data for surveillance purposes, as they would not need to go through foreign countries’ or intermediaries’ data management protocols to access this data.51

As detailed in this section, the nature of the surveillance being conducted by some states, appears to run counter to African and international human rights standards. In a number of instances, it fails to offer sufficient protection to individual human rights such as privacy and data protection and freedom of expression. Moreover, it contravenes the necessity and proportionate principles on the conduct of communication surveillance.52 These international best practices provide that determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent (Principle 6); the obligation on governments to make enough information publicly available so that the general public can understand the scope and nature of its surveillance activities (Principle 9); the requirement for states to establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance, with such oversight mechanisms having the authority to access all potentially relevant information about state actions (Principle 10).53 As will be exemplified in the Results section, by ignoring these safeguards, state surveillance in Africa has harmed various rights of journalists, HRDs and opposition politicians, and undermined their proclivity for participation in social and public affairs.

---

52 Necessary and Proportionate https://necessaryandproportionate.org/principles/
This study set out to establish the impact of surveillance on democratic participation in Africa. This section presents the results of how human rights defenders (HRDs), civil society organisations, activists, journalists, and political opposition leaders experience state surveillance and how it affects their rights, political participation, and private lives.

4.1 Manifestations of and Experiences with Surveillance

Study findings show that governments have used different forms of surveillance on their citizens, including physical surveillance (87%), interception of communication (85%), accessing and sharing collected personal data (64%), as well as closed circuit television (CCTV) (50%). Other methods mentioned by the respondents included social media monitoring, mobile phone location tracking, hacking of mobile phones, and messaging and email applications, monitoring of financial transactions, surveillance through networks of family and friends, and aerial surveillance through drones.

Majority of the study respondents (65%) reported having been victims of state surveillance, with only 7% asserting that they had never experienced any form of surveillance, while 28% were unsure whether they had been surveilled. Respondents acknowledged that several African governments had invested heavily in acquiring the surveillance technology and software to facilitate their surveillance operations, while many of the laws required telecommunication service providers to facilitate monitoring and interception of communications. The collection of personal data through mandatory SIM card registration and issuance of national IDs was also mentioned as facilitating state surveillance.

4.1.1 Physical Surveillance

Several respondents reported having been subjected to physical surveillance that included being monitored and trailed by undercover security and intelligence officers. This form of surveillance was reported to have occurred in all the study countries.

I first knew I had been surveilled when I gave a talk four years ago. After the talk two agents from the state intelligence services approached me and issued a warning. This was then followed by a leaked list of people under surveillance which included me. A reliable source informed me that the list was primarily designed to intimidate and silence government critics. Academia, Tanzania.

I was subjected to physical surveillance and this was clear because in my travels around, I could see similar faces behind me at unusual places. My phone also produced a suspicious sound during calls which showed it had been bugged. I am now selective in terms of choosing meetings that I attend. I have also become very careful on what I eat at public functions in order to guard against poisoning. Male journalist from Zimbabwe.
I was surveilled on the phone and physically. I have often been revealed [to] the contents of my telephone conversations which I believed to be private. My phone was seized and searched - this is the first thing that they seize when you are arrested. And several times I have been alerted in the street by strangers who reported that they had noticed a person watching me, following me and making phone calls or sending messages by phone to report on my actions and movements. Political party activist, Cameroon.

It is now close to four years. Every time I go out of my house, there is a motorbike behind my car everywhere I go. Also, I don’t have the right to leave my country. Political party activist, Rwanda.

In countries such as Ethiopia, Rwanda, Tanzania, Uganda, Zambia and Zimbabwe some respondents indicated that they had been trailed by cars and motorcycle riders. Some suspected that vehicle tracking devices had stealthily been installed in their vehicles, devices or watches without their knowledge.

I was “gifted” a brand wrist watch by a gentleman who claimed to be my fan and follower. A few months later, I was involved in an accident that looked organised. Due to the suspicious nature of the accident I consulted friends including those that work in state intelligence. After [a] series of questions, it was later realised that the wrist watch I received was a transmitter device and that I was [being] monitored. Civil society activist, Zambia.

When I am arrested, oftentimes my gadgets come back when they had tracking devices. Political party activist, Uganda.

Some governments were reported to have deployed close contacts of their victims, including household workers, colleagues, friends, spouses, family, neighbours, foreign journalists, local community leaders and government administrative officers to regularly monitor and report on the activities of the person targeted by the state. This was reported by respondents in Kenya, Nigeria, Rwanda, Tanzania, Uganda and Zambia.

As a way out for my family I had to make them understand that if anyone asks any question about me, just deny that you don’t know me. This is the same reason I have to lock my friendship to prevent people from seeing who my friends are on Facebook. Journalist, Nigeria.

Other physical surveillance tactics that have been deployed include the use of state operatives to infiltrate target organisations disguised as employees; attendance of organisation activities as guests; and agents masquerading as employees of utility companies (water, electricity, telecommunications, etc.), ordinary civilians, students, bar/pub patrons, or motorcycle (boda boda) riders, or street traders to enable them access and monitor targets, their homes or offices.

Respondents also noted that sometimes, state agents disguised themselves as tenants in residential areas close to where the target resided to closely monitor and establish their target’s routines, movements, phone behaviors, among others.

One time some security officials asked to talk to me and after commenting on my online activities, they offered to accompany me to my home. They took me to my place without the need to ask me for directions in a gesture of showing that they knew my home and everything. Journalist, Ethiopia.
4.1.2 Interception of Communications

Even before the enactment of laws and policies enabling interception, many African countries were engaged in the surveillance and interception of communication. Several respondents reported having noticed that their communication was being monitored or intercepted. The most prevalent method reported across all countries was the monitoring, interception and recording of phone conversations. Further, state agencies in Cameroon, Kenya, Mozambique, Nigeria, Tanzania and Uganda were also reported to have gained access to personal data held by telecom operators, such as location data, call data, and mobile money records.

I don’t really know how they do it ... because when they arrested me I found them with my voice calls I had with my interviewees in the story I had published. That made me sure that they had intercepted my communications. Blogger, Rwanda.

I learnt that security agencies were listening to my calls when people I used to call would be arrested the following day. While being tortured, the recordings of our conversations would be played or sometimes they were told what I said when talking to them. Political party activist, Uganda.

The day I was arrested someone directly sent a photo via WhatsApp to my dad, even before the family was informed. And my daddy didn’t have that contact, had never had a conversation with the person, it was an unknown number and after that he didn’t communicate with my dad any more. This makes it clear that people have his number, know everything that is going on in my family and follow him very closely without him knowing who they are. Political party activist, Cameroon.

Since 2018 I have been the target of the state mainly because I am an active critic and human rights defender in my country. I received active threats because of my activism, they wire-tapped my communications to listen to who I am talking to up to today. In December 2019 I was kidnapped by my country’s security service agency at midnight. I was tortured inside the building of the Ministry of Home Affairs, forcing me to reveal who is “paying me” to do what I am doing and my connection with opposition political parties and high profile activists in my country. Government critic, Tanzania.

Some respondents only suspected being surveilled when they experienced reduced call quality, coupled with odd sounds, noises or overlapping voices during specific phone calls.

Many times in conversation with journalist colleagues and social activists we had our calls interrupted without any explanation. Sometimes we hear voices and noises from outside our conversations. The most incredible thing is that this is not common when the conversation is with a relative or personal friend from another profession. Journalist, Mozambique.

We always noticed that in our phone calls we would hear echoes. And some of my team observed and suspected they were physically followed, especially whenever we published new investigations targeting influential business persons, the head of government, and the ruling political party. Respondent, Tunisia.

Other aspects noted by respondents included attempts at hacking their social media, messaging and email applications (Ethiopia and Uganda); cloning of Android phones; news reports of state surveillance (Kenya, Rwanda and Tunisia); government admission of surveillance (Tunisia), leaking of phone call recordings (Zambia), and delayed receipt of text messages (Zimbabwe).

---

54 Tunisian security forces target journalists covering anti-austerity protests https://ifex.org/tunisian-security-forces-target-journalists-covering-anti-austerity-protests/
In addition to phone tapping and physical surveillance, I have experienced multiple attempts of hacking. Someone from the government, once again, informed me that my accounts are targeted to be hacked and I changed my two-factor authentication with a foreign number. Then I kept receiving notifications of attempts to access my Facebook, Gmail, Whatsapp, and Telegram accounts. They only succeeded in hacking Telegram for some time but I recovered it after a while. They succeeded in hacking the Telegram channel because I forgot to put on two-factor authentication. Journalist, Ethiopia.

I have been surveilled by the state because of my activism. My phone has been tapped, my blog and social media was being monitored. I have also been physically followed by civilian-looking people whom I don’t know. However, I became certain it was surveillance when I was jailed in 2014. Police had transcribed [a] copy of my phone conversations and blogpost contents. Civil society activist, Ethiopia.

State agents have sometimes resorted to theft, disguised as search and seizure, often without a warrant, of targets’ digital communication devices.

Unknown people broke into my house in the middle of the night ... and took all electronic gadgets and when I tracked my iPhone (using Find My Phone) it was found at the Chieftancy Military Intelligence (CMI) offices. Lawyer, Uganda.

### 4.1.3 CCTV Surveillance

In the recent past, the use of closed-circuit television (CCTV) to conduct surveillance has gained prominence in the respective countries with significant investment and deployments reported in the streets of the major cities across the different countries. In 2014, the Kenya government deployed 2,000 CCTV cameras in the main cities with support from Safaricom and Huawei. Similarly, In Cameroon, a National CCTV Command Centre was launched in August 2019 to monitor 2,000 CCTV cameras installed by Huawei, with an additional 7,000 expected at a later date.

In Nigeria, a USD 470 million CCTV project initiated in 2011 in Abuja stalled due to funding shortages, which proved a challenge to its roll-out and implementation. In Zimbabwe, a bomb explosion in 2018 led to increased deployment of CCTVs in rallies addressed by the president and in state buildings. In Uganda, Huawei has since 2019 been installing a CCTV system whose command centre is at the police headquarters in Kampala, with 83 monitoring centres and 522 operators with a second phase launched in 2020 integrating the installation of facial recognition cameras to be connected to 107 monitoring centres at various police stations in major towns and municipalities.

We learnt from July last year that the regime does not like being spied on when we secured and released CCTV footage of them surveilling my nephews. The agents involved, we later gathered, were transferred to various places. So to fight back we have had to install CCTV at home and work and we hope this works as a deterrent. Journalist, Zimbabwe.

In the private domain, respondents from the countries under review indicated that CCTV surveillance was increasingly being deployed in business establishments such as banks, private offices, residential areas, homes, and automobiles. Likewise, drones had emerged as a surveillance tool that could be used for aerial surveillance. Some of the respondents indicated that they were wary of the use of this form of surveillance on them.

I restrict my movement a whole lot because I can’t tell the place that is being surveilled digitally. For example, if somebody that they are monitoring is careless to frequent a particular bank they can subpoena that bank to give them CCTV footage. Journalist, Nigeria.
A key challenge that has emerged is the absence of a legal framework for the deployment of CCTV surveillance, and the opacity of the responsibility and structures for their management. Also, where there is a proposed policy such as in Kenya, the provisions of the proposed National CCTV Policy entrench privacy derogation rather than safeguard the right by, among others, requiring installation of CCTV in public areas and requiring owners to integrate their CCTV cameras with, and grant links to state security agencies. Moreover, it is yet to be apparent how the cameras that have since been deployed in public areas have been utilised across the countries to solve criminal cases, which is usually the basis for their deployment. Nonetheless, there are some worrying reports. For instance, Huawei facial recognition technology was reportedly used to crack down on government critics in Uganda, leading to the arrest of over 836 suspects during protests in 2020.

### 4.2 Effects of Surveillance on Civic Engagement and Democratic Participation

This section reviews the effects of surveillance as experienced by the respondents on their rights, relations, health and work and their ability to participate in democratic processes.

#### 4.2.1 Undermining the Right to Freedom of Expression and Access to Information

The rights to freedom of expression and access to information are critical to meaningful democratic participation and civic engagement. The inability to freely express oneself has a direct impact on democratic participation since it limits an individual's engagement in political discussions and the capacity to influence others, especially during periods of political contestation, as well as limiting engagement in civic spaces.

> It affects your freedom and you attend a meeting where you are supposed to debate [but] you censor yourself. It leads to self-censorship in other words. Male legal service provider from Rwanda.

The fear of repercussions associated with surveillance curtailed the rights of individuals who had been victims of surveillance to freely express themselves. Several respondents indicated that they had been forced into self-censorship in several ways, despite the desire to express themselves on various platforms. Respondents indicated that they exercised restraint, were less vocal, and limited their comments and opinions especially in conversations or debates touching on political affairs both online and offline.

> I have not voiced my opinion online in a while. Lately I have practically disappeared from social media. Female Journalist from Nigeria.

Some respondents indicated that they had stopped speaking openly, freely or sharing their opinions publicly, especially on social media, during interviews, public meetings, or in the presence of strangers or government officials. These respondents indicated that in such situations, they had to think critically about their options, select the opinions they shared, and choose their words carefully. These approaches were replicated on social media, where respondents indicated the exercise of greater caution, conscious of the possible repercussions from state agents. Likewise, while on phone, respondents indicated their difficulty in airing certain opinions and avoiding communication with strangers generally.

> I used to be a regular panellist on most of the political shows e.g the Friday Spectrum on Radio One was a place where I enjoyed engaging, would never miss for as long I am in town, the Fourth Estate [TV programme] we were the pioneers and I used those fora to engage on democratic affairs but now they no longer invite me for fear of revocation of their licences. Civil society activist, Uganda.

---


Some journalists indicated that they exercised self-censorship in their coverage and reporting of stories and as such, did not publish politically sensitive opinions, posts or articles. A respondent from a radio station indicated that they no longer aired programmes with political content. Also, respondents from Tanzania indicated that they no longer shared unofficial statistics due to legal restrictions.

I no longer post or comment on politics as much as I used to. I avoid even sharing posts with harsh critics or what may be interpreted as violent. I heard and saw many people being prosecuted and facing jail time for a Facebook post. Female government critic, Tunisia

In the course of their work, some respondents indicated that they had faced retaliatory actions for expressing their views and opinions, including online extremism and negative propaganda characterised by false and malicious articles written about them and posted online to discredit their work; being trolled and attacked on social media; being branded a hater of government.

Because [state intelligence agents] are there [online] using fake profiles, they control what we write and make threats disguised as simple dissenting opinions. In the worst case, as I have experienced a few times, agents connected to the regime told me directly that the posts would have serious consequences. Journalist, Mozambique

My social media platforms are constantly monitored and if I post anything about government the state machinery are always deployed to discredit me by calling me [a] homosexual, rapist, child abandoner and so many other things just to make the public biased about me. Civil society activist, Uganda.

In other instances activists were kicked out of TV shows and property owners would outrightly refuse to host them in their premises if they sought for house rental services.

When I know that government officials are present, such as a minister, and I know that I’m regarded as an enemy, it would make me censor the things that I am going to do or say, knowing that I don’t want to upset the system, because I don’t want my words or actions to be misconstrued. Online, I saw a lot of malicious messages, that even affected my team, they would report fake articles about me, so we had to mind what we post online because we don’t want to be misquoted. We had to overthink what we post so that we could be prepared for the repercussions. Civil society activist, Zambia

Some media stations had also received threats to have their licenses revoked due to hosting government critics.

As an open government critic, I was chased from NBS TV where I was the panellist for the Frontline political show. The government said I am dangerous and that if NBS TV management does not drop me their licence will be revoked. I have been the Board Chairperson for the Citizens' Coalition for Electoral Democracy in Uganda [CCEDU] since 2019 and from that time CCEDU has not been allowed to function well. First the staff were questioned on why I was made the chairperson, also during the 2021 general election, CCEDU was denied observer status. Government critic, Uganda

On a positive note, some respondents indicated that state surveillance had not muzzled their freedom of expression.

I have chosen to let them enjoy the surveillance as I live my best days. I have adopted safer digital methods and applications. Civil Society activist, Kenya.

Some respondents indicated that they continued to speak the truth about what is going on in their countries; and continued to communicate and voice opinions freely offline and on social media. Others indicated that they had adopted innovative ways of communicating and expressing political opinions, including through the use of comedy, satire, coded language, metaphors and sarcasm.
4.2.2 Infringing on the Right to Privacy of Communications

Surveillance by its nature intrudes on the privacy of the individuals. It is also a means through which fear is instilled in political activists, the opposition, HRDs and the public. Notably, surveillance affects individuals as it involves digital and physical observation of individuals to monitor their activities. According to the United Nations High Commissioner for Human Rights, the right to privacy is not only impacted by the examination or use of information about a person by a human or an algorithm. Rather, even the mere generation and collection of data relating to a person’s identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk.

Some of the respondents interviewed indicated that as a result of the surveillance they had experienced, they were more careful about how they used their phones. In particular, most opted not to share sensitive information or work-related information through phone conversations.

In terms of receiving information, I am unable to receive certain phone calls. If it is someone I know I will use someone else’s phone number to call the person and since I am often alone until I am unable to get somebody who I can borrow their phone to make a call that means communication will be delayed. So, it now appears like I am a procrastinator. Female Journalist from Nigeria

Some indicated that they were generally reluctant to use their phones or largely avoided phone conversations or messages. Further, some used phones of third parties to communicate in order to circumvent surveillance, while others no longer stored any phone numbers on their phone handsets.

It has affected my communication with individuals working for the government. I opted to communicate using a messaging app rather than using telco lines. Female civil society activist from Kenya.

With respect to communication online including on social media, some of the respondents reported that due to surveillance, they had changed their online behaviour. Several indicated that they kept a low profile online and had significantly reduced their online activities, lost interest in social media platforms and digital communication channels and were generally reluctant to use the platforms due to security concerns. Some respondents indicated that they had exited WhatsApp groups or closed their social media accounts altogether.

I am very resistant to interact with people until I am sure my communication is secure. Civil society activist, Tanzania.

Overall, surveillance had some negative effects on the ability of respondents to use digital communication channels - some stopped using the channels to communicate altogether, or restricted their communications. Further, it had increased their cost of communication, which arose from travelling to physical meetings, purchase and deployment of security software, and the cost of internet bundles for use in digital communications.

It forces me to incur some extra costs in communicating because I have to use software that assures me of my privacy but these services are not free. You have to pay for them. Journalist, Tanzania.

The study also found that respondents implemented various practices to protect the privacy of their communications. Some of the measures adopted included: being more careful with communication; keeping communications confidential, for example by setting chats to disappear after conversations and only sharing information on a need to know basis; limiting conversations on phone; regularly changing communication channels; and avoiding discussions or sharing sensitive information such as activism plans, meeting details, and information sources through phone conversations. Others reported increased use of online channels to communicate due to their inability to hold or attend physical meetings, or as in the case of Uganda, the suspension of Facebook meant respondents had to use other social media networks.

It has only prompted me to be more careful. For example, there are some conversations I don’t have casually on social media. There are things some people are trying to talk about with me, I take the conservation off social media and use platforms that have end-to-end encryption such as WhatsApp or Telegram just to be careful. Male civil society actor from Nigeria.

4.2.3 Curtailing Freedom of Assembly and Association

The right to freedom of assembly and association is intricately linked to the rights and ability to freely express oneself, seek information, and mobilise. The curtailment of these freedoms can be felt in the individuals’ withdrawal from active engagements with peers, their representatives to parliament and other political actors. The rights to assembly and association are limited for those who are victims of state surveillance.

It has isolated me from many people, for instance, the fear to associate with Bobi Wine, who has been my friend for many years but now you don’t know what case the state will come up with just by seeing me with him. People also fear associating with me. In an organisation where I was a board chair, we had to change the colour (from red) for fear of being misinterpreted as an organisation advancing the People Power movement. Legal service provider and civil society activist, Uganda.

The ability to organise and mobilise for activities, especially political meetings, was among the aspects of the rights to association and assembly that were adversely affected by state surveillance. Some respondents had resorted to organising meetings online as opposed to physically, and only with trusted individuals, which affected the reach and effectiveness of such meetings and the mobilisation efforts of such actors.

By forcing the victims of surveillance to be mistrustful of both strangers and even some of their own associates, surveillance had severely affected the ability of such individuals to do their work (in the case of journalists and HRDs) or to mobilise for causes they were passionate about (e.g. HRDs and opposition politicians). Such individuals had adopted anti-social behaviour, were careful about people they associated with, cut down on public meetings including those of a social nature.

Many people that I knew cannot even say hello to me when we meet at the supermarket. And because I want to keep them safe, I choose to stay away from so many people. Political party activist, Uganda.

For activist organisations and political parties, state surveillance had affected the willingness of citizens to attend meetings, and as a result, they were more selective about where they held meetings. Many avoided hotels and other venues frequented by state operatives and often held meetings in homes, and had to carefully vet physical meeting venues to ensure they were safe and secure.

The knowledge that surveillance is possible has made me to be more cautious especially when we hold meetings and we have events. If it is a virtual event for example, we don’t share the venue carelessly. Even for a physical event, we don’t share the venue openly, we try to make sure that only people who have been selected to attend the event have the links to the venue or the address. Male civil society actor from Nigeria.

Some of the victims of surveillance had remained active in promoting political processes and democratic participation and supporting their parties and causes. However, some respondents reported that, as a survival mechanism, they had been prompted to profess support for the ruling party or to shun association with any political party.

It makes me worried and very picky with whom I associate because it may be very consequential. I worry that everything can be interpreted wrongly. Therefore, it has pulled me back. For some time until 2018, it was literally impossible for me to organise meetings because security officials sabotaged meetings. Civil society activist, Ethiopia.

64 The colour red is widely associated with the opposition People Power movement led by Robert Kyagulanyi, a.k.a. Bobi Wine.
Moreover, some of the respondents indicated that they had faced additional restrictions from authorities that limited their rights to freely associate and assemble.

> After the 2021 general elections, our partners produced the findings of the election observers. A few days to the launch, officials from [the government-run] NGO Bureau reached out to us [and] asked why and what we wanted to launch. They went ahead and asked the landlord to chase us from our offices and now we do not have an office. Government critic, Uganda

Common restrictions include denial or permits to organise protests or meetings; and interference, disruption, sabotage, or halting of their operations and activities by state agents.

### 4.2.4 Curtailing Freedom of Movement

The respondents surveyed indicated that state surveillance had affected their right to freedom of movement. While the state had directly imposed restrictions on the movements of some actors, for the majority it was the fear of being trailed and monitored, or even arrested, that prompted them to cut down on their movements.

> I am so security conscious to the extent of being paranoid at times. I once missed a flight because I never wanted to be at the airport early for fear of being under scrutiny. Civil society activist, Zimbabwe.

Other respondents reported that restrictions had been placed on them preventing them from leaving the country, while others had been forced into hiding or had fled from their home countries.

> As I don’t have the right to leave my country, I cannot visit my husband and kids ... whom I haven’t seen for 11 years. Political activist, Rwanda.

Some respondents had adopted measures to protect themselves, including being more alert about their surroundings.

> If I am entering this compound and I know I must provide my personal details I restrain from places I would like to go because I know I will provide my ID details. Male legal service provider/advocate from Rwanda.

Others respondents used aliases for instance on taxi-hailing applications like Bolt and Uber, switched off location services on their devices to limit tracking, and stopped disclosing their locations on social media.

> Because I have come to understand that I am being monitored... even the location app on my phone I have it turned off. I also don’t book a [taxi] ride for myself any more, I ask a friend to help book the ride and I make sure at the end of the trip I pay cash. Journalist, Nigeria

Further, some respondents indicated that they limited their movements and stayed indoors most of the time. They only visited safe locations and avoided political rallies, protests, or walking out at night.

> I am now very cautious about what I post online and I do not move around alone late at night or go for walks alone, even in my neighborhood. I am also cautious about openly sharing my views on the state of political affairs especially when I am around colleagues I am not very familiar with. Civil society activist, Zimbabwe.

Lastly, to limit opportunities for their personal data being captured, some respondents opted to avoid visiting places where national IDs were required, or which had CCTV cameras. Capturing and triangulating such data could help state agents establish patterns of such individuals’ movements and activities.
4.2.5 Effect on the Work of Organisations

State surveillance had several adverse effects on the work of organisations, making it difficult to achieve their goals including gathering information and mobilising for activities. Staff of organisations that had been targeted said they avoided wearing branded organisational clothing in public.

* I get the idea that someone is listening to me and may plan an attempt on my life because of the work I intend to do or I am conducting. This sometimes delays the achievement of my goals because I can’t communicate immediately on the phone. I must find another way to communicate, and even then, not [from] just anywhere. Male Journalist from Mozambique.

Some organisations, including political parties, had been affected by the disruptions of their activities by state actors, including being evicted from their offices by landlords at the request of state officials. Such actions had affected the relationships of the organisations with other government officials who they engaged with in their work.

* The government intimidates our action[s]. I am more afraid of the state than of bandits. Journalist, Mozambique.

Further, the costs of running the organisations had gone up, due to the high cost of the investments made towards implementing safety and security measures. Also, additional funds were required to undertake the complicated recruitment processes due to the needed background checks. At the staff level, organisation staff indicated that they lost precious energy and time worrying about surveillance, and as such felt controlled and less free in undertaking their work. Some respondents indicated that their organisations had scaled down their work, while others indicated that they no longer worked on governance issues.

On the positive side, some respondents indicated that despite having knowledge of possible surveillance activities, they had not changed their work, life, or employers. Other respondents indicated that they were aware of surveillance and had taken steps to mitigate its effects. Some of the measures included strengthening their human rights advocacy and activism. Others had become more careful, conducting regular due diligence and risk analysis to assess possible security threats and filling up risk matrices before undertaking their activities. Additionally, they had implemented security practices such as avoiding storing sensitive information in devices.

4.2.6 Impact on Personal Life and Relations

The impact of surveillance goes beyond affecting peoples’ ability to meaningfully participate in democratic processes, to their personal life and relations. Individuals who were targets of state surveillance reported that their relationships with their family, friends and society were affected. In particular, many respondents lamented their lack of a social life as they could no longer make new friends, visit their old friends or family members, invite them to their homes, meet them freely, or be seen with them in public. They also avoided public events, even of a social nature.

* The people I knew ... some have received threats of arrest and intimidation so they hesitate to keep in touch with me. Other people- childhood and teenage friends - no longer have contact with me because they are afraid of being tracked. My children no longer have friends because their friends’ parents have prevented them from seeing my children for fear of being watched. It affects everyone. Political activist, Cameroon.

Personal and professional relationships have been affected, and many victims of state surveillance said they were lonely, having lost many friends.

* My family members never tag me and they don’t even write about me on social media because they already know that I am a security risk to them. They don’t even put up my picture anywhere to even show that they know me. I am living this ostracised life both online and offline. For the offline part, I avoid going to my siblings’ homes and they don’t come to visit me. I also don’t receive visitors in my house. It is not a pleasant way to live for me and I have come to understand that I can’t live my life anyhow. Female journalist from Nigeria.
Respondents indicated that they restricted their social media engagements with friends and family, by among others, abandoning social media altogether, limiting acceptance of friend requests, or preventing themselves from being tagged in photos by friends and family. Many had also stopped posting personal information or photos on social media. The respondents cited the discomfort of friends and family in their presence, their fears of jeopardising their own security and the safety of their friends and families, or a general suspicion as to whether some of them could also be spies. As a result, many of the respondents indicated that they felt isolated, ignored and avoided by their close friends and family members.

In family relationships, I try not to cause struggles for my family because I know they suffered in my first arrest. Some old people in my neighbourhood have a jail stigma about me. Male activist from Tunisia.

Some respondents indicated that their friends and family who interacted with them did so with a lot of restraint and limited their communications with the respondents who, due to the nature of their work, were perceived as high risk state surveillance targets. Some friends and family distanced themselves from associating with the respondents because they had been warned by state agents to keep away from the state targets. Meanwhile, some of the respondents faced logistical challenges getting their friends and families to use secure communication channels to stay in touch.

I have lost friends because of the physical surveillance. Some people feel less security for being seen with me. Civil society actor from Ethiopia

The level of mistrust of friends and family extended to romantic relationships. Some of the respondents reported that they did not trust their romantic partners, and as such, they avoided such relationships generally, ended them, or limited the information they shared with their partners, including for the partners’ safety. Other respondents reported that their families, including their children, faced stigma from their neighbours which affected their relationships.

A friend of mine, also a journalist, once told me that he split up with his girlfriend because he found out that she used to spy on him. He met the girl at a conference of diplomats, not knowing that she was a secret agent. They dated and later he found out that she was a secret agent and even collected information about him and his colleagues. Since he told me about this affair I have been afraid to meet new people, including answering certain questions to my wife about the activities I am carrying out. Male journalist from Mozambique.

Despite the challenges, some of the respondents indicated that they had learnt to live without meeting or communicating with friends. For others, their experiences had strengthened their spirituality and relationship with God, their relationships with loved ones and with some friends. Others had continued to benefit from their good relationships and reputations through which unknown people continued to share with them information about possible dangers and threats to look out for and avoid. However, other respondents continued to live normally as they opined that their work was not illegal and as such they had not been affected by surveillance.

4.2.7 Effect on Psychological Well-Being

The research found widespread fear among the respondents, including their families, friends and colleagues as a result of the surveillance they had experienced, or due to the apprehension of ongoing or future surveillance. Respondents reported that surveillance of their communication, lives and work had affected their psychological well-being and mental health in various ways. The mental toll of surveillance had resulted in constant and increased feelings of anxiety, anguish, stress, worry, depression, paranoia, fear, isolation, danger, risk, hurt, and insecurity. Consequently, these states had led to a deterioration in the quality of their lives.

I just quietly stay on my own, this makes some people think I am a snob. It leaves this mixed feeling about me. Meanwhile, people don’t know what I am battling with. Respondent, Nigeria.
There was widespread fear among respondents of retaliation or repercussions for expressing opinions, in the form of threats, intimidation, harassment, arrest, attacks, abduction, detention, prosecution, death, and making their family, friends and associates targets of state action.

Respondents also indicated their fear of communicating and speaking openly with family, colleagues and friends. Other respondents reported that they feared meeting new people or strangers, and eating at public functions. Apprehension was reported by some respondents who worked for civil society, who feared that their organisations might be infiltrated by state agents. Moreover, some had stopped sharing information on human rights violations for fear of repercussions to their work.

_The mental toll, anguish and near recline into depression because of the intrusion in my life has really affected my association with other people. The surveillance has created a sense of suspicion and disharmony among my team. For instance when I was arrested in 2020, some of the security agents told me that one of my staff was giving them information._ Legal service provider and civil society activist from Uganda.

The family and friends of state surveillance targets were also affected by the surveillance and its effects on the targeted individuals. Some of the respondents reported that their families and friends had been traumatised by their arrest and detention, and were always fearful that the individual may lose their life as a result of their work.

_As we do our work, our families are constantly scared for our lives, not sure whether we will be able to return home. As a result most people who have been involved in governance issues are slowly getting off the radar for fear factors._ Civil society actor, Uganda

As a result of the surveillance of the state targets, some members of their families and friends were afraid of communicating, engaging, being seen in public, or being associated with those who had been targeted for surveillance. The families and friends were also afraid of being implicated in the work of regime critics, being seen as part of groups “antagonising the government” or being labelled as “enemies of the state”. This was due to the fear of the repercussions that could arise from such association (whether real or imagined) such as arrest, victimisation by state agents, losing their jobs or business opportunities, attracting surveillance or monitoring.

Respondents who had been spied on indicated that they had as a result become more suspicious and did not trust any person they interacted with generally, including some family members, friends and colleagues. The mistrust was extended to the devices that they used, whose safety from surveillance was constantly in question.

_Surveillance makes you suspicious of your old friends because you don't know who they are friends with. Then there are all the new ones that are potential dangers, claiming to sympathise or empathise, to share what you have experienced and yet they sound [like] potential spies. So I tend to be suspicious of everyone, except that I know that I have been arrested for no valid reason, and even without a reason I can always be [re]arrested. So I remain cautious._ Political activist, Cameroon.

As a result of their experience, some respondents indicated that their mindset had changed after being surveilled. Some expressed that they had lost confidence, were skeptical of, or no longer believed in democratic processes such as elections or governance reforms. Others reported that they were more radicalised after their experiences including arrest, while others had opted to remain silent on political issues to attain peace of mind.

Others who had undergone surveillance indicated that they were neither afraid of surveillance nor intimidated by the repression of their governments. Consequently, they had gained courage and were motivated and inspired to speak out and expose the abuses of power by government officials.
4.3 Mitigation Measures adopted to Cope with Surveillance

Several respondents indicated that they had adopted various measures to adapt to or mitigate the effects of surveillance in order to continue with their activities. On digital security, the respondents indicated that they had adopted various measures. These include: switching to secure platforms with end-to-end encryption such as Whatsapp, Telegram, Signal, Proton mail, Linux, secure (HTTPS) websites, secure emails; adopting better security practices e.g. two-factor authentication, strong passwords, use of VOIP calls, encryption of data, and VPNs; adopting cloud backup and storage of their information; avoiding the use of public WIFI Hotspots; and ensuring physical security of the digital devices, including computers and phones.

Further, some proceeded to invest in regular digital security checks and assessments of their devices and ICT infrastructure; enhancing organizational information security systems; training for staff at their homes and offices; and the performance of background checks on all persons that access organisational information and networks such as staff, volunteers and consultants.

Other practices adopted included: changing email addresses and phone numbers regularly; setting chat conversations to automatically disappear; switch off digital devices e.g. phones and computers during meetings; and keeping off certain social media platforms e.g. Facebook, Instagram and WhatsApp.

On physical security, the respondents indicated that they had adopted various measures. These include improving the measures to ensure personal safety such as learning basic security practices such as taking precautions; investing in security measures; calculating movements; situational awareness and vigilance of environment; use of security surveillance cameras in cars, homes and offices; conducting regular security risk assessments of homes and offices; and adopting risk-based approaches in the management of personal and organizational security.

Others indicated that they held sensitive conversations and physical meetings in secure locations away from the presence of unknown people; avoided large gatherings; avoided driving around alone in the evening or at night; exercised care in the persons they engaged in meetings; partnered with in-country and regional human rights defenders organizations to access assistance and safe house in case of emergencies; and, engaged and informed close confidants and lawyers whenever they are travelling within or outside their countries. Moreover, some respondents indicated that they had grown thick skins and continued living normally.

With respect to communication, the respondents indicated that they had adopted various measures. Some of the measures adopted included: revising their internal communication strategies; limiting sharing of sensitive information on communication platforms; investing in better and secure ways to communicate; avoiding direct phone calls; and communicating anonymously. Respondents also changed their practices on social media, including by not sharing personal information on the platforms; halting usage of insecure platforms; and limiting contact with strange or unknown persons.

Some made changes to how they expressed themselves. These included ensuring that anything they said or wrote online could be repeated in public without fear of repercussions; use of code language when speaking on phone; and, limiting speaking in public spaces and contributions to certain debates.

At work, some of the noted changes included reporting factually and objectively on stories and issues of public interest; highlighting incidents and cases of state surveillance to the public; building confidence and inspiring trust among colleagues; and suing government agencies over their surveillance practices and abuses. Unfortunately, some respondents who were journalists, indicated that they had opted for freelance work and had stopped working on political stories for safety reasons or until safety was guaranteed.
4.4 Discussion of Study Findings

The research findings show that surveillance has become a principal threat to digital rights in the countries under study, a weakening force to civil society and independent voices, a bane for opposition politicians, and ultimately a driver of authoritarianism. The study establishes that both physical surveillance and digital surveillance have been prevalent in these countries for several years. Yet digital surveillance is expanding in scope, and includes the use of spyware, drones and video surveillance (CCTV), as well as social media monitoring, mobile phone location tracking, and hacking of mobile phones, messaging and email applications.

Government critics including leading opposition leaders, human rights defenders and activists who do human rights and governance work, as well as investigative journalists, are prominent targets of state surveillance. Indubitably, these states routinely use surveillance as a tool for political control and instilling fear, thus threatening democratic practices, as has been found elsewhere. The stated reasons for conducting surveillance are to ensure national security and tackle terrorism, cybercrime, riots, hate speech and violence. However, as the study shows, state surveillance primarily targets political opponents, dissidents and critics, human rights defenders, activists and journalists simply because of their work. This indeed supports a key finding of the study that, one of the objectives of surveillance in the region is to enable the state perpetuate censorship by silencing or stifling criticism especially about state accountability and corruption; instilling fear and intimidating activists and critics that are perceived as threats to the regimes; and discrediting these individuals and limiting their reach and influence.

The key enablers for surveillance are the laws which have been mirrored from country to country. Some of the enabling provisions in these laws are ambiguous and wide in their scope of application, and grant the relevant authorities excessive powers to carry out privacy interference with minimum control measures that would lead to accountable and transparent enforcement. While democratic participation is based on free will and freedom, the law has been instrumentalised to intimidate and to carry out arbitrary arrests and detention, prosecution and persecution of individuals.

Indeed, laws in most countries studied do not emphasise the judicial oversight role over lawful interception, which gives the state and its agents the leeway to conduct surveillance with insufficient oversight. This limited oversight over surveillance activity, where the actions of those who conduct illegal surveillance remain shrouded in secrecy with limited accountability for their actions, or redress for victims of surveillance, remains of concern. Such concerns are exacerbated in countries, such as 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.

The overreach effect of increased surveillance across the region is the curtailment of rights to freedom of expression and opinion, access to information, and diminished appetite for participation in democratic processes, including in political debates and social media conversations. The victims of surveillance and those who closely work with or associate with them, have tended to take an overly cautious approach due to fear of repercussions such as being arbitrarily arrested, prosecuted and detained. The rights to freedom of expression, assembly and association are intricately linked to the rights and ability to freely express oneself, seek information, and mobilise. The curtailment of these freedoms can be felt in the individuals’ withdrawal from active engagements with peers, their representatives to parliament and other political actors. Previous studies in the region have found that surveillance laws and practices cause different actors to self-censor and refrain from exercising their fundamental human and democratic rights.

The individuals whose proclivity to participate gets lowered is not limited to those that are directly subjected to state surveillance; it extends to individuals who know of the existence of surveillance against other persons and the general public. In turn, it is apparent that state surveillance is undermining independent media, weakening the mobilising and oversight power of the political opposition, and diminished civil society’s role in engendering good governance.

---

Among the most worrying findings of this research is that human rights and governance actors who knew about or were targets of surveillance had significantly changed their behaviour and engagement in the online domain. One of the “democratising effects” of the internet was that it had provided a safe and alternative engagement platform that could help circumvent and diminish the repressive state’s control over the offline means of communication, thereby enabling greater organising and expression of dissenting opinions. Yet, autocrats in the region have appropriated the power of digital technologies to stifle dissent and to ramp up their own capabilities to snoop on, punish, and silence critical and dissenting forces. Indeed, as it has turned out in the majority of the countries studied, ICT has been turned into a tool of repression in the hands of autocrats, who are using it to impose further restrictions on civil liberties.

The surveillance of individuals, some of whom have been arrested, violates many of their rights and freedoms, including those necessary for democratic participation. In Tanzania, the multiple arrests, trials and convictions of citizens due to their use of the digital space has stifled democracy in the country. There were similar occurrences in Uganda where human rights activists were arrested following surveillance of their communications and movements. Over time, citizens in some countries have been gripped by fear of being arrested, detained and prosecuted due to their expression or association. Such fears are heightened where state surveillance has, in addition to targeting particular individuals, expanded to threats of death to the victims and their family members. Such threats are primarily intended to scare and discourage critics and dissidents from engaging in political activities such as public criticism of governments and leaders.

Invariably, the nature and extent of surveillance activity tends to mirror the overall governance situation in a country, including the level of respect for the rule of law, constitutionalism, democratic principles, human dignity, and digital rights. Abuse of surveillance is rife in countries with high levels of impunity for rights violations and a low level of accountability for the actions of the government and its institutions. In virtually all countries studied, not only has surveillance become commonplace but the right to communicate anonymously in digital spaces has been profoundly eroded through mandatory SIM card registration and creation of inter-linked databases for national ID, voters’ registers and other services provisions. Previously, the anonymity which individuals enjoyed in the online world was believed to make them feel empowered to speak up against powerful actors because of having less fear of repercussions. As it is, this is negated in an environment of perceived and real state surveillance.

Ultimately, surveillance has undermined the potential of the internet to boost political participation including for repressed individuals and groups. On the other hand, it has reinforced the power of autocratic governments who have appropriated technology’s power to entrench the self-serving needs of ruling parties and elites. It is clear then that the countries under study will need to enact strong laws on privacy and data protection, revise laws permitting the interception of communications so they are more rights-supporting and put in place strong oversight and accountability safeguards. Moreover, state oversight institutions such as parliament and the judiciary who are also under threat from rogue and autocratic executives will need to step up to not only defend and assert their independence, but to champion the respect for civil liberties and the digital rights of citizens.

---

67 Empowering activists or autocrats? The Internet in authoritarian regimes, https://www.jstor.org/stable/24557404
72 Death threats and repressive regimes: the activists fighting for online freedom in Africa, https://www.wired.co.uk/article/african-governments-repress-online-expression
5.1 Conclusions

From the foregoing, it is evident that state surveillance had led to massive effects on the lives of the respondents surveyed, their colleagues, family and friends. These effects and changes have affected their interactions online and offline and severely diminished their ability to effectively participate in civic engagement and democratic processes.

The interception and monitoring of communications, self-censorship, movement restrictions, infiltration of their organisations by state agents, disruption of activities by state agents, the fear of repercussions from the state, as well as the actual repercussions, were the major drivers contributing to the erosion of democracy and curtailment of rights, including to political participation. These have been aided by the existence of flawed surveillance laws, their abuse by state security agencies, the absence of comprehensive judicial and parliamentary oversight of state surveillance, increasing state investments in surveillance capacity, and autocratic governments keen on breaking the law to maintain their grip on power.

While state surveillance continues unabated, the respondents indicated that the continued advocacy, coupled with the greater investments in digital and physical security enhancement and training, use of secure communication channels, better situational awareness, and continuous security risk assessment were increasingly critical means to safeguard the security and safety of actors perceived as “enemies of the state”. What is also emerging is that despite state surveillance intensifying and becoming more invasive and inevitable as part of the arsenal of state repression, these positive practices and measures to enhance physical and digital security are not being widely practiced or employed by the specific groups under threat. Organisations, groups and individuals pushing back against state repression and demanding for state accountability must now rethink their physical and digital security if they are to survive the rapid onslaught by the ever-increasing number of autocratic and repressive regimes in Africa.
5.2 Recommendations
In order to restore respect for the fundamental human rights that have been undermined by the state surveillance, consequently affecting democratic participation, it is important that deliberate efforts are taken by various stakeholders, including government, civil society actors, the private sector especially communication service providers, and the media.

Governments and Parliaments
1. Repeal, amend or review existing laws, policies and practices on surveillance, interception of communication, biometric data collection, and limitations on the use of encryption to ensure compliance with the established international minimum standards on human rights and communications surveillance.
2. States without specific data protection laws, such as Tanzania, should fast track the enactment of standalone data protection laws so as to guarantee the right to data protection and privacy.
3. Countries with data protection laws such as Uganda and Kenya should also expedite the establishment and operations of independent data protection authorities and put in place clear administrative structures to guarantee their independent operations.
4. Appreciate and respect the independence and role of the judiciary in its exercise of the oversight role over the implementation of data protection and privacy laws to ensure warranted implementation.
5. Parliaments need to proactively check the excesses of the state and its agencies in surveillance and demand for accountability and transparency of the executive arms of government.

Civil Society
1. Engage in strategic advocacy initiatives including media campaigns and capacity building activities aimed at promoting data protection and privacy rights.
2. Continuously engage in legislative advocacy especially through participation in law-making processes by doing analysis of bills and submitting them to Parliament.
3. Engage in strategic public interest litigation through collaborative efforts to challenge laws, measures and acts that violate privacy rights and push for policies and practices reforms that uphold privacy.
5. Partner with the media to investigate, document, and expose data and privacy breaches such as unauthorised access, surveillance and non-compliance by data collectors, controllers and processors.
6. Adapt and take positive steps to overcome external threats from governments and other players by, among others, enhancing cyber security to protect organisations from digital threats.
7. Build capacity of their staff and the general in digital literacy, cyber hygiene, physical and digital security and data protection measures; new digital threats; and evolving surveillance measures and practices.
8. Strategically engage with states and their respective security agencies to reach complementary positions such as specification of limits for surveillance and interception of communications. This can potentially enable and enhance the protection and promotion of digital rights and freedoms.
Media

1. Dedicate human and financial resources to carry out investigative journalism on cases of illegal surveillance and interception of communication against citizens.
2. Continuously expose and report all cases of unlawful surveillance and interception of communications through various media platforms so as to push for accountability and transparency against the key perpetrators.
3. Build capacity of media staff in cybersecurity such as in the use of digital security tools to enable them to circumvent possible cases of digital surveillance and compromise of electronic gadgets by malware, viruses and bugs.

Telecom Companies and Internet Service Providers

1. Challenge laws, policies and directives that provide weak privacy and data protection and place undue intermediary liability obligations through utilising litigation in national and regional courts and other quasi-judicial processes such as tribunals.
2. Internally, develop and implement and strictly comply with privacy and data protection laws, policies and best practices in handling customer data, including sharing of the same with third parties.
3. Regularly publish, update and widely disseminate privacy policies and transparency reports and inform users about the collection, use, handling, sharing and retention of their data and the measures taken to protect their right to privacy.