AFEX Annual Report on the State of Internet Freedom in Africa - 2019
Annual Report on the State of Internet Freedom in Africa 2019

With Funding Support from IFEX
The publication is available for public use. It can be reused or quoted provided the African Freedom of Expression Exchange (AFEX) is appropriately referenced.

Published by the African Freedom of Expression Exchange (AFEX)
32 Otele Avenue, East-Legon
P.O. Box 730, Legon, Accra-Ghana
Telephone: +2333(0)2555327
Twitter: @AFEXafrica
Facebook: African Freedom of Expression Exchange (AFEX)
Email: info@afex.org
Website: africafex.org
About the African Freedom of Expression Exchange

The African Freedom of Expression Exchange (AFEX) is a continental network of some of the most prominent freedom of expression and media rights organisations in Africa that are also members of the global free expression network, IFEX. The network is currently made up of 15 member organisations spread across West, East, Central, and Southern Africa. Some of the members operate in more than one African country in a particular region. AFEX seeks to promote freedom of expression and human rights on the continent through advocacy and campaigns, capacity building to ensure effectiveness of members and other free expression groups in the region.

Our Member Organisations

Africa Freedom of Information Centre (AFIC)

Association for Media Development in South Sudan (AMDISS)

L’Association pour le Developpement Integre et la Solidarite Interactive (ADISI-Cameroun)

Centre for Media and Peace building (CEMESP)

Collaboration on International ICT Policy in Eastern and Southern Africa (CIPESA)

Freedom of Expression Institute (FXI)
Gambia Press Union (GPU)

Institute for Media and Society (IMESO)

Journaliste en Danger (JED)

Media Institute of Southern Africa (MISA)

West Africa Journalists Association (WAJA)

Human Rights Network for Journalists in Uganda (HRNJ-U)

International Press Centre (IPC)

Media Foundation for West Africa (MFWA)

Media Rights Agenda (MRA)
Introduction

With each passing year, the internet is increasingly becoming an important part of the lives of people living and working across the African continent. By September 2019, the world average internet penetration rate grew to an estimated 54%\(^1\) - in that same period, the internet penetration rate in Africa rose to an estimated 39%.\(^2\)

The International Telecommunications Union notes that, “overall, the proportion of all women using the Internet globally is 48 per cent, against 58 per cent of all men. More men than women use the Internet in every region of the world except the Americas, which has near-parity.”\(^3\)

Social media services and instant messaging applications (Apps) have brought convenience and affordability to the way people communicate. This affordability and convenience have propelled the internet’s popularity among Africa’s urban populations.

Africans use the internet for various purposes including for communication, entertainment, commerce as well as for the enjoyment of democratic rights such as access to information and participation in public affairs. This varied use of the internet to enhance the human experience is of utmost importance and is at the centre of debates to keep the internet open, accessible, and affordable.

Unfortunately, the rights of internet users in Africa and the rest of the world are under growing attack from a host of actors that include state actors as well as non-state actors such as corporations.

The year 2019 saw a number of multinational corporations face charges and investigations based on the abusive and non-consensual exploitation and monetisation of user data. The same year saw an increase in the number of governments that passed laws meant to restrict free speech and access to information in online environments. It was also the year that saw a spike in the number of African countries that experienced prolonged internet shutdowns or information controls.

While it is impossible to look at internet freedom related incidents from all of Africa’s 54 countries, this report will analyse the internet landscape in 10 African countries to identify common themes of how some African governments have chosen to deal with the internet within their respective geographical boundaries. The events selected for this report provide a handy reference to some of the major internet freedom incidents that took place in Africa in 2019. The report covers developments that took place in 2019 in Burkina Faso, Chad, the Democratic Republic of Congo, Nigeria, South Africa, Sudan, Tanzania, Uganda, Zambia, and Zimbabwe.

The report also seeks to provide recommendations to the AFEX network and partners on how to best advocate and lobby for an open, accessible, and affordable internet.

The first part of the report is comprised of country snapshots which are brief summaries laying out the main internet freedom related policies and incidents in each country. The second part of the report discusses the common internet freedom related themes. The last part of the report

---

provides recommendations aimed at equipping AFEX members for their work to keep the internet open, accessible, and affordable.

**Country Updates**

**Burkina Faso**

Burkina Faso is a landlocked country in West Africa with an estimated population of 20.6 million people. A former French colony, the country gained its independence in August 1960. Since 1966, the country has experienced several coup d’états leading to political instability that saw one former president stay in power for 27 years. Following civil protests that led to Compaoré’s resignation in take over, a transitional government was formed which manned the affairs until elections were organised that ushered in the current government led by President Roch Marc Christian Kaboré.

The years of political instability combined with military rule have negatively influenced Burkina Faso’s economic growth. It is therefore not surprising that only an estimated 20% of Burkina Faso’s total population has access to the internet. Since 2016, the Burkinabe government has been in negotiations with Huawei, a Chinese enterprise over the rollout of a fibre optic network at an estimated cost of around US$180 million. Once completed, Burkina Faso will have an estimated fibre optic network spanning 10,900 kilometres spread over the country’s 45 provinces. Initial phases of this project began at the end of 2017.

The rollout of fibre connectivity has led to a slight drop in the cost of internet connectivity in the country; however, the cost of accessing the internet remains beyond the reach of many. This is mainly attributed to the fact that like in most of Africa’s developing countries, the internet is accessed mainly using mobile devices that rely on mobile data and less on fixed line solutions.

From a policy perspective, the government of Burkina Faso has introduced and maintained laws and policies meant to tightly control the sharing and receiving of information in online environments. Two main developments stick out in this regard. The first relates to the amendments that were made to Burkina Faso’s Penal Code (Code pénal de Burkina Faso). According to government representatives, these amendments were meant to fight terrorism and organised crime, the spread of “fake news,” and suppress efforts to “demoralise” the Burkinabe armed forces. These amendments were effected on 1st August 2019.

Furthermore, Article 160.3 of the Burkina Faso Constitution establishes the Superior Council of Communication that is responsible for the monitoring of information shared in Burkinabe media and Internet. This Council is housed under the office of the President and is largely viewed as being set up based on the President’s interests and those of his ruling party.

---


The combined effect of the repressive amendments to the country’s Penal Code as well as the establishment of the Superior Council of Communication is likely to lead to an increase in arrests for information communicated over social media and other online platforms. At the time of writing this report, the researchers did not come across any arrests made in terms of the amended laws.

Chad

The Republic of Chad is situated in the North Central part of Africa with an estimated population of 16.2 million people. It is estimated that 75% of the population still resides in rural communities. According to World Bank statistics, Chad is classified as a low-income country. Estimates state that by the end of 2018 only 5% of Chad’s population had access to the internet. Despite these seemingly low figures, it is reported that Chad’s internet access rates grew by 90% between 2017 and 2018.7

Like Burkina Faso, Chad gained its independence from the French in August 1960. However, the post-independence peace was short lived as Chad experienced political instability including military rule and a civil war. In 1990, President Idriss Déby came to power and has led the country for the past 30 years.

During his prolonged tenure, President Déby has used national laws to consolidate his grip on the presidency. For example, in 2005 the Chadian government organised a referendum that led to the removal of presidential term limits meaning an incumbent president could stand for re-election for as many times as he or she wished.

In early 2018, a national conference recommended that the national Constitution be amended to extend presidential terms from 5 years to 6 years, with presidents remaining in office for a maximum of 2 terms. This would apply to President Déby and would essentially mean that he could remain in office until the year 2033. These proposed constitutional amendments led to nationwide protests, on 28th March 2018 the government retaliated by effecting an internet shutdown that lasted until around 27th July 2019.

During that 16-month period, Chadians could only access the internet and Applications such as Facebook, WhatsApp, and Twitter only by using Virtual Private Network (VPN) Apps and services. It is estimated that the total cost of this internet shutdown was at least $125 million, which is a lot of money for a low-income country such as Chad.

Chad is not new to internet shutdowns as there was also an internet shutdown in 2016 that extended over 8 months to protest the President voted into office for the fifth time. The country illustrates the close relation between political events and information controls and internet shutdowns.

The tendency to limit free expression online is a reflection of government efforts to clamp down on free expression in offline spaces as well. In 2019, the Chadian government used State security forces to clamp down on at least three separate demonstrations. In April 2019, the Minister of Security banned a planned protest against the shortage of butane gas organised by the Collectif Tchadien Contre la Vie Chère. 13 protesters were assaulted and arrested when the peaceful protest went on despite the ban on 25 April 2019.

---

On 1 June 2019, police fired teargas at people participating at a parade held in N’Djamena to commemorate the launch of a new opposition party Les Transformateurs. A news conference to launch the party was also banned by government authorities. In November 2019, a peaceful protest to demand the enforcement of a 2015 court order to pay compensation to former President Hissène Habré was disrupted after security forces fired teargas onto protesters.8

The Democratic Republic of Congo

The Democratic Republic of Congo (DRC) is a central African country that attained independence from Belgium in June 1960. This independence brought with it decades of political instability, civil wars, assassinations and prolonged military rule. The country has an estimated population of 81 million people, with only an estimated 6.2% of this population with access to the internet. The mobile penetration rate stood at 5.5% for the same period.9

The national telecom system remains one of the least developed in the region,10 but there has been a steady increase in the number of internet users. This is partly attributed to the expansion of the country’s telecommunications infrastructure that includes the expansion of a fibre optic network that will see for example, the Société Congolaise des Postes et des Télécommunications (SCPT) quadruple the capacity of optic fibre that is between the landing site and Kinshasa.

As more urban dwellers have come online, they have used the internet to safely share information in a rapid and affordable manner. The internet has played an important role in the organisation of demonstrations and other forms of civil action. When the DRC held a national election held in December 2018, the government shutdown the internet and blocked use of the Short Message Service (SMS) service.

The excuse the government gave was that it was promoting public order by preventing the spread and sharing of "fictitious results" on social media. This shutdown is estimated to have cost DRC between US$2 and US$3 million per day as a result to the limited access to the internet.

In the past, the DRC has not been hesitant in shutting down the internet with shutdowns recorded in 2011, 2016,11 and 2018 into 2019. One thing that these incidents have in common is that they coincided with significant political events, such as those relating to then President Kabila’s succession and elections.

The government acting through the Regulatory Authority of the Post and Telecommunications of Congo (ARPTC)12 most often issues orders to telecommunications operators to shutdown the internet. Mobile network operators and internet service providers operating in the DRC are compelled to comply with these orders as refusal to shutdown communications may lead to the abrupt suspension of an operator’s license.13 In addition to the orders issued through the ARPTC,

---

the DRC government may also rely on a communications law (Law 013/2002) to take control of the country’s communication facilities in the interest of national security or public defence.

David Kaye, the UN Special Rapporteur on freedom of expression issued a special plea to the DRC government to restore internet. In the same statement, Kaye points out that internet shutdowns are unjustifiable. He says, “A general network shutdown is in clear violation of international law and cannot be justified by any means.” Additionally, he states that “Access to information is crucial for the credibility of the ongoing electoral process. Shutdowns are damaging not only for people’s access to information, but also for their access to basic services.”

Nigeria

Nigeria, home to the biggest economy in Sub-Saharan Africa and a large population of about 201.8 million in 2019 has an individual internet use of 42%. Nigeria has a number of laws in its statute books that attempt to regulate social media and online activities. Some of these laws infringe on online rights, chief of which is the Cyber Crimes (Prohibition, Prevention) Act that was passed in 2015 and has been relied on to prosecute persons particularly journalists who publish articles criticising the government. Furthermore, these legal frameworks and the law are used by the State as tools to silence dissent. This goes against the basic tenets of democracy that include open debate and free expression.

A prominent example of the politicised interpretation of laws was the arrest of Omoyele Sowore in August 2019. Sowore who is with Sahara Reporters ran as an opposition presidential candidate in Nigeria’s February 2019 elections. The government charged Sowore with treasonable felony for using his social media and online platforms to call for protests in August 2019 against bad governance under the #RevolutionNow movement.

Nigeria has consistently attempted to regulate the online environment. In 2015, Nigeria attempted to pass the controversial Frivolous Petitions Prohibition Bill that was withdrawn in May 2016, following protests by citizens and advocacy by civil society organisations that include AFEX network members Media Rights Agenda (MRA), International Press Centre, and Media Foundation for West Africa (MFWA).

In March 2018, Nigeria introduced a widely controversial Hate Speech Bill before the Senate to tackle hate speech and defamation online. The move raised concerns of the possibility of its usage to stifle freedom of expression and silence government critics.

The Buhari-led government failed to show the same appetite for passing internet related laws when it refused to pass the progressive Digital Rights and Freedom Bill into law in March 2019. This draft law was the product of joint efforts between Nigeria’s civil society working with the Senate to produce a law that protects and promotes internet freedom.

In September 2018, Nigeria’s Federal Executive Council (FEC) approved the immediate commencement of the implementation of a strategic roadmap for Digital Identity Ecosystem in

---

14 UN expert urges DRC to restore internet services
Nigeria. According to the National Identity Management Commission (NIMC), the process will see the effective and efficient mass enrolment of Nigerians and legal residents in Nigeria into a centralized, secure National Identity Database. This identity database will be the basis for the rollout of digital identities in the form of the National Identification Numbers (NIN). As of January 2019, digital identities are increasingly becoming mandatory for transactions from, raising concerns of possible state surveillance.

In June 2019, the State Security Services initiated a nationwide crackdown on an undisclosed number of internet users who allegedly posted inciting materials on internet platforms. According to the SSS, “social media users were skewing Nigeria’s history to promote ethnic violence and tip the nation into crisis, a development it said must be urgently reversed through state interference.”

The Nigerian government has reportedly acquired and is using unspecified social media surveillance technologies that it uses in a non-transparent manner.

On 6 June 2019, the Nigerian Broadcasting Commission indefinitely shut down the operations of African Independent Television (AIT) for allegedly contravening the National Broadcasting Commission Act and Nigeria’s Broadcasting Code. Speaking at a press conference the NBC’s Director General stated that his Commission had repeatedly issued warnings to AIT’s holding company before the suspending its services. AIT was accused of being partisan and was presenting national issues in a divisive and inciting manner.

AIT challenged the suspension of its services at the Nigerian Federal High Court. The court ruled in AIT’s favour leading to the restoration of its broadcasting services on 8 June 2019. The suspension of AIT’s broadcasting services is worth including in this report about internet freedoms because a significant part of AIT’s broadcasting services are accessible on online platforms in addition to its traditional free-to-air services.

Sudan

Sudan has considerably developed infrastructure for internet access, including different service providers of broadband and mobile internet access. With a population of over 43,849,260 people, Sudan has mobile access to over 29.8 million. There is also an estimated 13.12 million internet users of 2019 and internet penetration of 30.9%.

For years, Sudan was under the firm rule of president Omar al-Bashir from 1989-2019. President Bashir was deposed through a coup. He currently stands accused of several international human rights crimes and crimes against with a warrant of arrest from the International Criminal Court. During his tenure, he enjoyed protection and solidarity of other African member states, who solidly refused to concede to the jurisdiction of the ICC over Sudan and a sitting president. During his tenure, fundamental rights and freedoms on expression, association, and assembly were gravely assaulted.


Ibid


AIT back on Air as court ordered NBC to restore license. https://businessday.ng/lead-story/article/ait-back-on-air-as-court-ordered-nbc-to-restore-license/
In December 2018, Sudan experienced massive protests linked to the economic challenges. Youths, organised groups, professional associations amongst others took to the streets of Khartoum protesting continued economic decline, unemployment, rising costs of basic goods and general frustration with the status of affairs. President Bashir responded with deploying the military resulting in the killing of hundreds of protestors. Protest organisers used internet and social media platforms that the government quickly cut off.

The internet shutdown and blocking of social media lasted for 68 consecutive days, with Facebook, Twitter, Instagram and WhatsApp outages beginning on the morning of 21 December 2018 and lasting until February 26 2019, according to NetBlocks internet measurements. During this period main internet mobile service providers, Zain, MTN, and Sudani could not provide access or connection to Facebook, Twitter, and WhatsApp. Users had to connect through a virtual private network (VPN). Internet access was further hampered by power outages during the protests, however there clearly were orders to shut down the internet.

The economic situation in Sudan has caused the price of internet access to skyrocket and become inaccessible to most citizens. As a commodity (oil) backed economy, the global decline in prices of oil affects the economy, resulting in increases of all basics. The inflationary environment affected costs of communication that became unaffordable for the majority of citizens. According to Freedom House (Freedom on the Net 2019), a month of fixed-line internet service can cost nearly half of the average monthly income in Sudan. This limits access to the internet by many.

Online expression is susceptible to monitoring, removal of content and self-censorship as individuals, and journalists fear arrests and prosecution under the existing criminal laws including the Law on Combating Cybercrimes of 2018. This law was enacted despite the existence of several others law which are similarly worded, including the Media and Publication Law (2009), the Cybercrime Act (2007), the National Security Act (2010), the Criminal Act (1991), and the Access to Information Law (2015).

The 2018 Cybercrimes law provides that “anyone who uses the internet, or any means of communications, information or applications to disseminate any news, rumour or report, knowing it is fake, to cause public fear or panic, threaten public safety and offence the reputation of the State.” In addition, the Law criminalizes “anyone using the internet or any communications or information means, to incite hatred against foreigners, causing discrimination and hostility” will face a two-year prison sentence.

South Africa

South Africa with a population of 58.8 million, is the second biggest economy in Sub-Saharan Africa. South Africa’s constitution guarantees rights such as freedom of expression, privacy and freedom of association. It is known to be the biggest economy in terms of internet use. According to the ITU individuals internet access use, South Africa has an internet use level of 56%. Affordable access to the internet has been as a major challenge to internet access in South Africa over a period of years marked with the #datamustfall campaign.

---

In a positive move to ensure affordable internet access, the regulator - ICASA introduced End-user and Subscriber Service Charter Amendment Regulations in February 2019. The pro-consumer interventions were seen to address affordability through usage notifications for consumers, ability to transfer mobile data on same network, rollover unused data and consumers not having to be charged out of bundle data rates when their data expired. Together with review of mobile pricing, South Africa will finally see auctioning of spectrum that had been a point of contention in the last decade. Following a ministerial directive, a roadmap on the sale of the spectrum had been set up which will finally see much needed spectrum on sale. The regulator is now overseeing the process after having a received an interdict to halt planned auctions in 2016 from going ahead with the auction will be overseeing the process

Hate speech is a major challenge in South Africa. The proposed Prevention and Combating of Hate Crimes and Hate Speech Bill is still pending. The Bill is, however, problematic as it may have a chilling effect on social media. In addressing hate speech and defamation online, the high profile case of Trevor Manuel vs Economic Freedom Fighters saw the law of defamation being apply to issue and interdict on the latter party over a tweet.

The most prolific challenge to state surveillance in 2019 was the successful challenge to Regulation on Interception of Communications Act (RICA). In September 2019, the amaBhungane Centre for Investigative Journalism and journalist Stephen Patrick Sole sued the state at the High Court of South Africa in Pretoria, having learned that law enforcement agents had spied on the journalist’s phone for at least six months in 2008. In a unanimous ruling, the Court declared that bulk surveillance activities and foreign signals interception by the South African National Communications Centre is unlawful and invalid. This was a landmark ruling on issues of interception of communications and state surveillance on which further jurisprudence in other African countries can be built on.

In May 2019, the High Court in Gauteng presided over a defamation case that arose from a series of tweets published by the Economic Freedom Fighters (EFF) opposition political party accusing former finance minister Trevor Manuel of corruption and nepotism. The court ruled that the tweets were defamatory and ordered that the EFF take down the offending tweet within 24 hours of the ruling, the court also ordered the political party to pay R500,000.00 (estimated US$28,000.00) in damages.

The EFF has instigated online attacks against journalists on at least two occasions in 2019. In March 2019, EFF’s leader Julius Malema made a Twitter post encouraging his party’s followers to harass Karima Brown a South African broadcaster. The tweet included Brown’s private mobile number. This came after Brown mistakenly sent a WhatsApp message intended for her work colleagues on another WhatsApp group that included EFF supporters, in her message, Brown encouraged her colleagues to “keep a watching brief” of an EFF event. Malema misrepresented the communication including death and rape threats.

24 ICASA asks public input on mobile data regulation. ITWeb https://www.itweb.co.za/content/mYZRXv9PVzJqOgA8
25 ICASA sets down the spectrum road. Charley Lewis. ITWeb https://www.itweb.co.za/content/rxP3jMBp2ElvA2ye
28 ALT Advisory, Social Media and defamation online: Guidance from Manuel vs EFF. https://altadvocacy.africa/2019/05/31/social-media-and-defamation-online-guidance-from-manuel-v-eff/
29 Abamthungan Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services Case No. 2597/2017
30 Trevor Manuel vs the EFF: High Court judgment https://www.politicsweb.co.za/documents/trevor-manuel-vs-the-eff-high-court-judgement
31 EFF court losses mount as Karima Brown wins battle, but faces criticism of her own. court-loses-mount-as-karima-brown-wins-battle-but-faces-criticism-of-her-own/
Karima Brown approached the South Gauteng High Court to seek relief on grounds that Malema’s actions were in contravention of the South African Electoral Act “by failing to ensure that journalists did not face harassment, intimidation or threats in the run-up to the May elections.”

The High Court ruled in Brown’s favour.

Tanzania

Tanzania has been termed ‘slowly becoming an internet predator’. This stems from a history of online surveillance, criminalisation of online communication and the use and abuse of the courts of law to stifle internet freedom. In 2019, Tanzania’s population was estimated to be 58.01 million with an the internet penetration rate of 45%. As of January 2019, 23 million people were active internet users being 38% of the total population. With specific focus on social media, 4.9 million people were active social media users. Out of this number, 4.4 million people were mobile social media users.

Despite the recorded increase in internet penetration, it can be noted that several laws and policies have also been passed which have a negative impact on internet access, internet use and freedom. The Cybercrimes Act that was passed in 2015 is one of the oppressive laws that the Tanzanian Republic has relied on to muzzle opposition and dissent or any criticising of the government. More recently the Electronic and Postal Communications (Online Content) Regulations of 2018 were passed which called for the licensing of bloggers and owners of other online platforms at a fee of USD$900.00. Such licensing requirements and exorbitant fees would only serve to infringe on the exercise of free expression by bloggers and content creators whilst also restricting the public’s access to information.

In March 2018, the Tanzania Communications Regulatory Authority (TCRA) launched a project to register the owners of 43.2 million active SIM cards using biometric technology. Following this, all SIM cards will have to be registered through biometric technology, using NIDA IDs or at least a NIDA registration number from May 1, 2019 and is expected to be completed by December 2019. Moreover, in January 2018, Tanzania commissioned a new electronic East African Community passport to replace the existing passport, set to be phased out by January 2020.

The e-passport contains the holder’s biometric information on a tamper-proof page, to curb fraud and ease clearance at immigration. This migration to biometric data poses a risk of continued state surveillance that would hinder exercise of rights on the internet for fear of repression. Such massive data collection also raises issues of data protection and privacy. While the constitution of Tanzania grants the right to privacy, Tanzania does not grant individuals extensive rights to privacy. This calls to action local and international rights groups to ensure that any use of such data falls within the ambit of the three pronged test on legitimacy, legality and proportionality.

In June 2019, Tanzania passed the Written Laws (Miscellaneous Amendments No. 3 of 2019) under a certificate of urgency that did not give ample time for the public to share their input into the Bill. These amendments were targeted mainly towards the Non-Governmental Organisations Act, 2002, the Society Act, Trustees and Incorporations Act inter-alia which raised an outcry from

---

32 Ibid
33 Mapping Trends in Government Internet Controls 2000-2019, CIPESA, 2019
34 Data Protection Africa - ALT Advisory: Tanzania https://dataprotection.africa/tanzania/
CSOs as it was seen as an attempt to cripple CSO operations particularly their ability to keep citizens informed and engaged on national issues of concern using the online media.  

It is worthy to note that Tanzania has also been employing more or less the same strategies as its fellow African countries to regulate the internet and exercise of digital rights. The challenge that needs to be overcome is that the internet, especially social media has been viewed by governments as a tool that is being relied on by ‘enemies of the state’ to spread false news and incite public violence. This therefore places the onus on CSOs to promote a paradigm shift and advocate for the protection and promotion of human rights.

In June 2019, a verified Twitter account belonging to Zitto Kabwe was compromised; several tweets expressing for Tanzanian President Magufuli were sent out from that account. At the time the tweets were sent out, Kabwe did not have access to his Twitter accounts because he did not have access to his laptop or mobile phone. This may indicate state sponsored hacking abilities.

Uganda

According to the International Telecommunication Union, individual internet use is less than a quarter amongst the Uganda population - 23% to be precise. Other estimates place Uganda’s internet penetration rate at 35%.

The year 2019 marked 33 years of President Museveni’s rule over Uganda. In those 33 years, Museveni and his government have continually relied on restrictive laws to silence dissenting voices as well as free expression in the country. Additionally, Freedom House found that the ruling party has retained its rule “through the manipulation of state resources, intimidation by security forces, and politicized prosecutions of opposition leaders.” As the use of technology has increased in urban Uganda, the government has used laws to silence any dissent that has emerged online.

2019 marked the one-year anniversary of taxes levied on the use of social media services accessed through Ugandan internet networks. Government introduced the tax in 2018 under the guise of boosting national revenue as well as to curb the sharing of ‘gossip’ and other malicious content online. However, the Ugandan government’s forecasted income from the tax failed to materialise, what the tax led to is a drop in the number of internet users as people opted to stop using the internet.

According to findings by the Collaboration on International ICT Policy for Eastern and Southern Africa (CIPESA), in the first year of the internet tax, Uganda’s internet user base shrunk by at

---


36https://twitter.com/zittokabwe/status/1144168557938454528


least 5%. The Uganda Communications Commission (UCC) confirmed the reduction in the number of daily internet users.

The Ugandan government has reiterated that the tax will stay in place despite the negative outcomes. Part of the population has resorted to the use of VPN services and applications as a way to avoid paying the tax that currently is about 200 Ugandan Shillings per day.

In July 2019, journalist turned pastor Joseph Kabuleta was arrested for posts he made on Facebook where he called to President Museveni as “a gambler, liar, and thief.” Kabuleta also posted that President Museveni’s son, Major Kainerugaba Muhoozi was making moves to position himself as the presidential heir.

On August 1, 2019, Dr Stella Nyanzi, an academic and human rights activist was convicted and sentenced to 18 months in prison for cyber-harassment against President Yoweri Museveni after she referred to him as a “pair of buttocks.”

Kabuleta and Dr Nyanzi were both charged in terms of the Ugandan Computer Misuse Act of 2011. Sections 24 and 25 of the Computer Misuse Act have been repeatedly criticised for unjustifiable criminalising legitimate free expression and criticism of government.

Another cause for concern is the group of experts that was convened in 2017 for surveilling Ugandan social media posts and usage. This group of experts was convened under the Uganda Media Council. The operations of this group are not clear and it is unknown whether they are still fully functional but the possibility of their existence and operation no doubt continues to have a chilling effect on the use of internet and social media in Uganda.

Zambia

As one of the stable democracies in Southern Africa, Zambia has seen successive changes in government since independence in 1964. These successive changes have enabled the deepening of democratic constitutional practices, but equally the entrenchment of power by the ruling elite through extension of constitutional term limits and third term interests.

The current government has been accused of eroding democracy and fundamental freedoms. Internet freedom in recent years has improved, according to Freedom on the Net 2019. However, there are major trends of concern, which include the increased censorship of journalists and users of social media networking sites (SNs), the increased costs of communications, proposals to impose social media taxes, and unclear legislative frameworks and policies on cybercrimes and cybersecurity.

---

42 Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%, https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/
44 Why Joseph Kabuleta was arrested https://www.newvision.co.ug/new_vision/news/1503451/joseph-kabuleta-arrested
45 Joseph Kabuleta picked up https://www.independent.co.ug/joseph-kabuleta-picked-up/
50 Lunga erodes Zambia’s democracy, https://mg.co.za/article/2019-09-06-00-lunga-erodes-zambias-democracy/ (last accessed 18 February 2020)
At least 5.1 million people enjoy internet access, while mobile access subscriptions are at 12 million, which represents about 75% mobile phone penetration rate. Several companies provide mobile telephony and data services, and several other internet service providers. There is significant liberalization of the internet and associated spectrum. Equally, the licensing process for such providers appears largely unencumbered.

Zambia’s policy and legislative framework on internet regulation and use is contained in varying laws including Electronic Communications and Transactions Act (2009); Information and Communications Technology Act (2009). Other critical laws remain in draft form such as the Cyber Security and Cyber Crime Bill (2017), Electronic Commerce Bill (2017) and the Data Protection Bill (2017). The draft Bills have several versions and it is not clear which one is official. The proposed Cyber Security and Cyber Crime Bill have provisions of concern that are likely to undermine freedom of expression. The Bill criminalises “any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person.” Based on past cases of arrests of individuals for expressing themselves on social networking sites, there is real apprehension that this Bill if enacted will lead to stifling of online expression.\(^{51}\)

In late 2019, Zambia proposed to introduce a tax on all web based communications platforms, those usually deemed over the top (OTT) services. This tax would affect users of Facebook Messenger, WhatsApp, Skype, and Viber. The specifics of the law were not public, raising concerns about the lack of transparency in policy formulation in Zambia. If the tax is imposed, over 2,280,000\(^{52}\) million users of Facebook for instance will be affected. In addition to social media tax, proposals to tax online streaming services, like Netflix have been mooted.\(^{53}\)

There are concerns of online surveillance by the government. Secure communication and anonymity is compromised with requirements for individuals to register the SIM cards. While there is no evidence of internet surveillance per se, Citizen Lab, listed Zambia as one of 45 countries worldwide using Pegasus, a spyware software used to target human rights defenders, media practitioners, and journalists.\(^{54}\)

**Zimbabwe**

Zimbabwe is a country in southern Africa with a population estimated to be at 14.5 million people. Despite persisting economic and political problems, an estimated 59% of Zimbabweans have access to the internet, mainly through their mobile devices. This mobile device based access to the internet has promoted the access to and use of social media Apps such as Facebook and Twitter along with instant messaging Apps such as WhatsApp. This usage pattern is further entrenched through the cheaper pricing of bundled mobile data packages, which encourage an App based access/ use of the internet instead of access to the general, open internet.

\(^{51}\) Sean Tembo, the leader of the opposition Patriotic for Economic Progress party, was arrested for a social media post, which questioned President Lungu’s mental state, March 2019. Chishimba Kambwili, the leader of the National Democratic Congress, was arrested on charges of defamation after a video went viral in which he allegedly insulted the president. August 2019,  
\(^{52}\) NapoleanCat, https://napoleoncat.com/stats/facebook-users-in-zambia/2020/01 (last accessed 18 February 2020)  
This has led to a situation where Zimbabweans use the internet to organise mass actions against government as was seen in the #ThisFlag movement that gained popularity in 2016. There was some renewed hope in the ruling party when long-time President Robert Mugabe was forced out of office in November 2017, this optimism quickly turned into frustration and subsequently public protests against the government.

A series of nationwide protests was planned for January 2019 against a hike in fuel prices. In a bid to disrupt the coordination of these protests, the government ordered an internet shutdown that would last from 15th -21st January 2019. During that week, Zimbabwe experienced total internet shutdowns on two separate days. The rest of the time, there were targeted shutdowns against social media Apps and websites such as Facebook, Twitter and WhatsApp. during this period of the partial or targeted shutdowns, many internet users had to resort to the use of VPN Apps and services.

The week-long internet shutdown ended when MISA Zimbabwe, a member of the AFEX network, collaborated with the Zimbabwe Lawyers for Human Rights to challenge the legality of the internet shutdown at the High Court in Harare. The court application challenged the government's use of the Interception of Communications Act as justification to shutdown the internet. The court challenge also sought a court order stating that internet shutdowns are an unjustifiable breach to the fundamental rights of free expression and access to information that are enshrined in Zimbabwe’s national Constitution.

The High Court in its ruling held that the internet shutdown was illegal because a Minister who acted without the President’s authority ordered it. The court’s order was as a compromise that ended the internet shutdown without examining the legality or constitutionality of internet shutdowns. In theory, the President of Zimbabwe may in future order the shutdown of the internet.

The Zimbabwean government still relies on existing laws such as the Criminal Law (Codification and Reform) Act, as well as the Access to Information and Protection of Privacy Act (AIPPA) to restrict free expression as well as access to information respectively. Like in previous years, 2019 saw a number of arrests based on the information people shared online mainly on the grounds that the information undermined the authority of the president, however, none of these arrests led to any convictions or detentions. The arrests were therefore, persecutory in nature and meant to chill overall freedom of speech online.

Cross-cutting Internet Rights Issues

Having looked at the significant developments in each of the focus countries, this part of the report focuses on the common themes that are evident in the way that each of the analysed countries has dealt with internet related rights.

**Continued use of statutory laws to criminalise information shared online**

By far the main threat to the enjoyment of internet freedoms on the African continent is the continued existence of statutory laws that criminalise free speech. Criminal law codes and penal codes are still used with varying degrees of outcomes. In Zimbabwe for example, none of the charges levied against people who share anti-government information online have led to any convictions, but in Nigeria and Tanzania anti-free expression laws have been used to keep government critics detained for long periods.
In addition to existing Penal Codes, African governments are introducing various laws and policies that seek to regulate use of the internet and use of internet related services. In other instances, countries will introduce policies such as the Ugandan social media tax or Tanzania’s licensing fees for bloggers. This regulation of the internet has given governments one more justification to take restrictive measures against their citizens’ right to free expression.

**Rise in information controls**

The year also saw an increase in the number of internet shutdowns recorded across Africa and the world in general. As outlined in the country profiles above, some African governments have resorted to using internet shutdowns as a means to control the sharing of and access to online information. According to Access Now, at least 14 African countries were recorded to have shut down internet or imposed partial network restrictions in 2019. These countries include Algeria, Benin, Cameroon, Chad, Democratic Republic of Congo, Egypt, Eritrea, and Ethiopia. The rest are Gabon, Liberia, Malawi, Mauritania, Sudan and Zimbabwe.55

Government sponsored shutdowns are usually justified under the guise of maintaining the public order or safety, national security and purported curbing of “fake news.” It is not surprising that internet shutdowns are mainly associated with political events such as the holding of elections as well as to diffuse efforts to organise attempts to hold public demonstrations against the government.

Internet shutdowns are an unjustifiable infringement of fundamental rights of expression, access to information, freedom of assembly and association. They have, accordingly, been condemned by key United Nations representatives as a gross violation of international law.56 The condemnation of the use of internet shutdowns has discouraged some governments from using total internet shutdowns as a way to stop the spread of information.

This may be one reason why authoritarian governments resort to partial internet shutdowns that target and interfere with access to specific services and Apps such as Facebook, WhatsApp, Twitter and YouTube. Other forms of emerging information controls are in the form of slowing or throttling of internet speeds in a manner that renders the use of the internet futile due to the failure to access services due to slow internet speeds.

**Access and Affordability**

One of the direct factors that have kept internet penetration low in the 10 countries covered in this report as well as other African countries in general, is the lack of infrastructure. The internet runs on infrastructure that ranges from mobile network towers, optic fibre as well as power sources needed to operate the gadgets for example, phones and computers that people use to access the internet.

Civil wars, low national incomes, and general mismanagement of national resources has meant that investments into upgrading and extending national ICT infrastructure networks are sidelined for other more pressing issues such as the provision of food, healthcare and education services. In undemocratic countries, national resources are funnelled to military operations and national security organs that are often used to prop the ruling party.


This lack of consistent and planned investment in national ICT networks means that internet availability is often concentrated in and around urban areas as well as along the major roads that connect a country’s urban centres. This has left rural populations behind when it comes to internet access, further widening the digital divide between urban and rural areas. Furthermore, the lack of investment by African governments has left a vacuum that foreign telecommunications corporations such as China’s ZTE and Huawei have been quick to exploit. ZTE and Huawei are two of the top three telecommunications firms working across Africa. See the illustration below.

Map of ZTE, Huawei, and other Chinese telecommunication companies involvement in sub-Saharan Africa.

This lack of investment in cheaper, more widespread and efficient telecommunications means that internet access costs remain exorbitant and beyond the reach of the majority of citizens in the countries profiled in this report. According to the 2019 Affordability Report, in Africa 1GB on mobile data costs is 7.12% of the average monthly salary. This is exacerbated by the sale of bundled mobile data or internet access that is linked to specific websites, Apps, and services. This commodified and compartmentalised access to the internet has skewed internet users’ understanding of what the internet is.

---

59 Alliance for Affordable Internet, Mobile Broadband Pricing, https://a4ai.org/extra/mobile_broadband_pricing_usd-2019Q2
Conclusions

The internet has become an important part of the lives of people living and working across the African continent.

Africans use the internet for various purposes including for communication, entertainment, education, commerce amongst other. Social media networks such as Facebook and Twitter have provided platforms where people can interact and also participate in public debates.

However, as citizens, journalists, bloggers, social and political activists use these platforms to demand accountability from duty bearers and other actors, they are coming under attacks. Strategic Lawsuits Against Public Participation (SLAPP) are on the rise to put fear in journalists, activists and citizens. There is therefore the need to ensure that measures are put in place to protect the rights of individuals online.

Recommendations

Below are a number of recommendations that various stakeholders may consider to improve internet rights in Africa:

Governments

- Repeal legislations that repress internet rights and desist from passing such laws.
- Take appropriate measures to make the internet open, accessible and secure.
- Undertake broad-based consultation with media, civil society and other relevant stakeholders in the formulation of laws and policies related to digital rights and freedom of expression.
- Commit to resource relevant security agencies to successfully investigate and punish abuse of digital rights and freedoms, irrespective of the perpetrators’ clout.
- Improve transparency and responsiveness in the provision of information about violations under investigation.
- Facilitate the activities of CSOs and media organisations that monitor violations of online free expression.

Regional and international inter-governmental organisations (ECOWAS, SADC, AU, UN etc)

- Develop and strengthen diverse mechanisms for sanctioning states, which resort to violations.
- Co-ordinate and deploy strong, international, and public condemnation of States involved in the violation of free expression and digital rights.
- Facilitate the visits of UN and AU Special Rapporteurs on Freedom of Expression to monitor and review digital rights ecosystems on the African continent.
- Support the capacity development of civil society, media organisations, regulators and other relevant governmental agencies on ways to safeguard digital rights and freedoms.
Civil Society Organisations

- Focus on championing repeal of repressive laws, and the passage of human rights centred policies and laws, to ensure the protection and promotion of human rights.
- Engagement with policy makers should strategically take into account the existent political economy that shapes responses to internet freedoms by the state.
- In cases where laws are used to repress the freedom of expression, strategic public litigation should be taken up. This may be a useful tool in cases of internet shutdowns as was demonstrated by the Zimbabwe 2019 litigation.
- Continue monitoring, documenting and reporting internet shutdowns and engage in evidence-based advocacies on the dangers of internet shutdowns. Tools such as those offered by Open Observatory of Network Interference (OONI) and NetBlocks that record instances of internet shutdowns are recommended.
- Include work on internet accessibility and affordability as they remain the biggest hurdles to internet use in Africa. Research from the A4AI has repeatedly linked the lack of adequate ICT policies to the high cost of the mobile internet data. Civil society actors in Africa must therefore, continue to advocate for ICT policies that result in the reduction of internet access costs.
- Champion enabling policy environments and encourage competitive and diverse markets to ensure affordability of internet services.
- Actively engage in consultative processes to addressing affordability to ensure all concerns are taken into account in policy development. This policy advocacy may include but not be limited to pushing for policies that promote telecommunications service providers operate in a country; there is a higher chance that pricing and the quality of service will be better than in countries where there is a monopoly in the provision of telecommunications services.

Internet Service Providers and Telecommunication companies

- ISPs and other industry players should uphold the rule of law by challenging unlawful requests from governments.
- Develop and adopt clear due diligence mechanisms among telecommunication operators, especially ISPs to manage illegal Internet shutdown orders and other unusual requests made by Governments.
- Prioritise telecommunications infrastructure provision in underserved populations and geographic locations to help bridge national and local inequities in digital resources and opportunities.
- Build and make available resilient digital solutions that will make it more difficult and cumbersome for government to resort to violations such as Internet shutdowns and unwarranted surveillance.