DIGITAL RIGHTS IN AFRICA 2017 REPORT

PARADIGM INITIATIVE

DIGITAL RIGHTS IN AFRICA REPORT 2017

Good for Business: Why Private Sector Must Work With Citizens, Civil Society for Digital Rights

Introduction

The first edition of our Digital Rights in Africa Report (2016), titled "Choking the Pipe: How Governments Hurt Internet Freedom on a Continent That Needs More Access", rightly characterized 2016 as the "Year of Internet Shutdowns in Africa". As at the time of its publication in December 2016, the year had seen 11 incidents of network disruptions and/or Internet (applications) shutdowns across the continent, for reasons as diverse as to prevent examination malpractice, citizens' protests, unofficial dissemination of election results and promulgation of hate speech online.

In 2017, the African digital rights landscape had three major themes dominating discussions across the continent – continued Internet shutdowns, attacks on press freedom, and pushback against digital rights abuses. The wave of Internet shutdowns, which increased significantly in 2016, continued in 2017. The year also saw widespread attacks on press freedom across the continent, and pushback by citizens and organizations against governments' digital rights abuses. Although 2017 witnessed Internet shutdowns in Ethiopia, Mali, Senegal, Somaliland (autonomous region of Somalia), Cameroon, Democratic Republic of Congo, Morocco and Togo; and state-sponsored attacks on press freedoms, it is also important not to lose sight of the demonstration of the power of citizens to push back at repressive actions of governments directed at violating their rights to privacy, Internet access and freedom of expression. The changing target of arrests of citizens exercising their right to freedom of expression also came to the fore. In 2016 there were widespread arrests of ordinary citizens for exercising their right to freedom of expression online, while in 2017, journalists – including bloggers – became the major targets across the continent.

Across the world, there was renewed emphasis on "Business and Human Rights", focusing on the role of telecommunications companies (telcos) and Internet Service Providers (ISPs) in implementing state surveillance and Internet disruptions. Hitherto seen as mostly unwilling participants in digital rights violations, the role of telcos and ISPs in digital rights violations in Africa, and the rest of the world has received attention by civil society actors.

Across Africa, a shift was also seen in how citizens responded to violations of their digital rights. In addition to direct recourse and appeal to international agencies, African citizens are exploring alternative options. Citizens across the continent have taken recourse to in-country or regional legal action to defend their digital rights. There is now a greater emphasis on the role of African institutions such as the African Union (AU) in arbitrating human rights on the Internet. Citizens have boldly approached the courts in various cities across Africa for legal interpretation of national laws concerning media and Information and Communication Technologies (ICTs). Some successes have been recorded in this endeavour and progress is being made with efforts in defence of digital rights within the continent, in addition to the previously observed recourse to international human rights organizations outside the continent. International advocacy is now part of a broader strategy which commences at local organisations that are the first lines of observation, defence and action around digital rights in Africa.

Trends in Digital Rights in Africa 2017

1. Rise in citizen pushback against digital rights abuses and legal victories

As noted in our 2016 report, although the year 2016 was unprecedented in the scale of digital rights abuses on the continent, there was also substantial citizen pushback. This was particularly seen in Zimbabwe where citizens explored other ways to mobilize for protests, thus defeating the government's shutdown of WhatsApp. The year 2017 witnessed an intensification of vigorous citizen pushback against digital rights abuses in Africa, particularly through the courts. In Cameroon, a coalition of civil society organizations instituted a case against the Cameroonian government for the ninety-three days of Internet shutdown the country experienced between January and April 2017[1]. Similarly, in Uganda, a civil society coalition also commenced legal action[2] against the Ugandan government for the social media clampdown surrounding the February 2016 elections. In Kenya, in response to a suit brought before it, a court declared section 194 of the country's penal code, which creates the offence of criminal defamation, unconstitutional[3]. In Cote d'Ivoire, the government withdrew a controversial Press Bill[4] in response to a petition by a civil society organization, while in Liberia, the President commenced action to decriminalize libel[5]. These developments were real gains for digital rights, as defamation, libel and press laws are prime instruments for the suppression of freedom of expression online in many African countries**.**

There is clearly more room for mass citizen action to force the hands of governments against digital rights violations on the scale of Internet shutdowns. Internet businesses are constantly under pressure from governments[6] to do their bidding, and the role of citizen power to restrain governments' tendency to violate digital rights has not been tested enough in Africa. There were however suggestions that in light of the spate of Internet shutdowns around elections in Africa in 2016, pressure from alarmed citizens who vigorously protested contributed to the government's' decision to keep the Internet on in Ghana[7].

[1] "MLDI and Veritas Law bring case before the Constitutional Council of Cameroon challenging Internet shutdown". May 4, 2017. https://t.co/tAa2y52Cjx
[2] "UCC Dragged to Court Over 'Unlawful' Social Media Shutdown in 2016 Elections, Date Set for Case Hearing". March 15, 2017. http://bit.ly/2mWnYyQ
[3] "Kenya: Court strikes down criminal defamation laws". Article 19, February 6, 2017. http://bit.ly/2kxMMJ5
[4] "Ivorian Government Withdraws Controversial Press Bill after MFWA Petition". Media Foundation for West Africa, June 8, 2017. http://bit.ly/2x94JFq
[5] "Major Boost for Free Expression as President Sirleaf Submits Anti-Criminal Libel Bill to Parliament". Media Foundation for West Africa, August 4, 2017. http://bit.ly/2hk7ekP
[6] Dave Lee, "Message encryption a problem – Rudd". BBC Technology, August 1, 2017. http://bbc.in/2wBi3EQ
[7] Eleanor Sarpong, "Yes, elections can be held in Africa without shutting down the internet". Joy Online, January 10, 2017. http://bit.ly/2vlGfXi

2. Increased recourse to local and/or regional African institutions for digital rights advocacy

While there has been significant pushback from African citizens and organisations against digital rights abuses on the continent, there seems to be a shift in the approach in responding to these violations. Although international human rights partners have played their part in the defence of digital rights in Africa, as seen in the examples of Cameroon, Uganda and Kenya, local courts and institutions are beginning to play a bigger role as the first line of defence for digital rights. As a case in point, in a ground-breaking move that was later shelved, the African Internet registry, AFRINIC, debated a proposal to withdraw Internet address resources[8] from African countries which shut down the Internet.

Also, more African organisations are embracing the African Court for Human and People's Rights (ACHPR), an organ of the African Union (AU) for the defence of human rights. On April 14, 2017, Tunisia joined Benin, Burkina Faso, Cote d'Ivoire, Ghana, Malawi and Tanzania in allowing its citizens and Non-Governmental Organizations direct access to the Court. The African Union (AU), under whose authority the Court operates, has recently strengthened its human rights focus, declaring the year 2016 as the "African Year of Human Rights" (with a focus on the rights of women) and the following decade as the "Human and Peoples' Rights Decade in Africa". Of key importance also was the African Union - European Union Human Rights Dialogue held on January 10, 2017, and the Joint Communique issued. Both the AU and EU "committed to promoting and protecting freedom of expression and the right of access to information in the digital age". They welcomed the ACHPR 2016 Resolution on the *Right to Freedom of Information and Expression on the Internet in Africa*, and emphasised that the same rights that people have offline must also be protected online.

3. A renewed focus on the role of business in human rights

The year 2017 saw a renewed emphasis on the role of business in human rights, especially in relation to digital rights. Although the understanding always existed that telecommunications companies and Internet Service Providers are sometimes complicit in digital rights violations, the year 2017 saw a major focus on this theme by civil society actors in Africa, and around the world. Civil society actors are no longer willing to accept the claim that Internet businesses are unwilling partners in Internet disruptions and other digital rights abuses. Rather, a number of leading civil society organizations have produced credible guidance[9] which Internet businesses can draw from in their engagement with governments.

[8] Kieren McCarthy, "Afrinic shuts down IP address shutdown over internet shutdowns". The Register, June 9, 2017. http://bit.ly/2vavtnl

[9] Dada T and Micek P, "Election watch: If Kenya orders an internet shutdown, will telcos help #KeepItOn?" AccessNow, July 26 2017. http://bit.ly/2xpzpl9

4. Increased attacks against press freedom

Journalists, society's bellwethers and conscience, increasingly do their work online to reach larger audiences, and have come under severe attack for it. The Internet has expanded the reach and amplitude of their message, and brought them into conflict with repressive regimes and hostile audiences within the continent. As fittingly expressed by Befeqadu Hailu, an Ethiopian journalist and a member of the Zone 9 blogger collective arrested in April 2014 and charged with terrorism, "the internet for journalism is now like the air you breathe. Without the internet, modern journalism means nothing"[10]. All across the continent in 2017, as this report documents, there were numerous stories of arrests, attacks and surveillance of journalists by their fellow citizens and governments. Among the most prominent stories in this regard are the reported mass surveillance of journalists[11] and blocking of several news websites[12] in Egypt, and the brutal arrests of citizens covering the Internet shutdown in the Al-Hoceima region of Morocco[13]. In Nigeria, there was an unprecedented number of arrests of journalists during the year. In fact, because journalists are probably the most effective users of the Internet as a form of mass communication in an official capacity, Internet freedom in many countries is synonymous with press freedom. It is hoped that the cases reported in the Digital Rights in Africa Report 2017 add to the growing voices against Internet (and press) freedom violations across the continent.

[10] Jonathan Rozen, "Journalists under duress: Internet shutdowns in Africa are stifling press freedom". August 17, 2017. http://bit.ly/2uVltOW
[11] Marwa Morgan, "How surveillance, trolls, and fear of arrest affect Egypt's journalists". Committee to Protect Journalists, June 12 2017. http://bit.ly/2xxmDnU
[12] Ahmed Aboulenein, "Egypt blocks 21 websites for 'terrorism' and 'fake news'". Reuters, May 24 2017. http://reut.rs/2yL3Fs0
[13] "Morocco obstructs coverage of Rif protests". Reporters without borders, July 23 2017. http://bit.ly/2wqQEp8

The United Nations Universal Periodic Review As An Index Of Human Rights In Africa

There is a growing realization among digital rights advocates of the need to halt the practice of viewing digital rights as an isolated objective; rather weaving it into the broader human rights discussion for greater advocacy success. Internet shutdowns, for example, have been proven to cause human suffering and deprivation because it cuts off millions of people from crucial financial, health and other services, as witnessed in the Cameroonian Internet shutdown this year. The human suffering occasioned by the shutdown was highlighted by the United Nations' envoy for Central Africa in his appeal to the Cameroonian government to restore Internet access[14]. By documenting stories of human suffering occasioned by digital rights violations, such as Internet shutdowns and arrests, into the broader narrative understood by the general human rights community and broader citizenry, digital rights advocates can pass their message across more effectively and achieve more success.

In this regard, the Universal Periodic Review[15] of the United Nations Human Rights Council, which reviews the human rights records of all UN members states, is useful as a broad barometer for human rights because countries who do poorly on other indicators of human rights, such as the rights of women and children, are also likely to violate digital rights.

Besides, Internet shutdowns result in steep economic losses for the country concerned. A coalition of digital rights organizations estimated the cost, to the local economy, of the 93-day Cameroonian Internet shutdown to be $4.5 million[16]. This conservative estimate did not include supply chain disruptions, losses due to a fall in investor confidence in the country and the incalculable cost of human suffering. Analysis by Paradigm Initiative and partners revealed that the first 30 days of the Cameroonian Internet shutdown cost the local economy FCFA 880m ($1,446,000). This sum could finance the total monthly municipal expenses across all 58 divisions in Cameroon, with enough left over to finance another 18 of such divisions[17]. Roughly speaking, this means the Cameroonian Internet shutdown's economic impact equalled the total monthly budgets of Cameroonian divisions with a population of 7 million working adults. The shutdown also severely disrupted Cameroon's budding technology industry[18], referred to as "Silicon Mountain". As a result of their round-the-clock need for reliable Internet access, tech start-ups in the cluster were forced to create an "Internet refugee camp" where business could proceed unhindered.

[14] "Cameroon: UN urges authorities to restore Internet in Anglophone regions. United Nations Regional Office for Central Africa (UNOCA)", April 13, 2017. http://bit.ly/2g4LI8o
[15] United Nations Human Rights: Office of the High Commissioner: "Universal Periodic Review". http://bit.ly/1BBFqdN
[16] "Cameroon counts losses after unprecedented Internet shutdown". Africa Review, April 24, 2017. http://bit.ly/2wDA9pG
[17] Babatunde Okunoye, "93 Days of Internet Shutdown in Cameroon: Advocacy Lessons Learnt". April 20, 2017. http://bit.ly/2opJk5Y
[18] Abdi Latif Dahir, "Reeling from an internet shutdown, startups in Cameroon have created an 'internet refugee camp'". Quartz Africa, March 28, 2017. http://bit.ly/2ncvh2a

FAST FACTS
INTERNET SHUTDOWN 2017

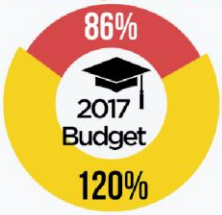
In **30 Days** the Internet blackout in the South West and North West regions of Cameroon has cost the country **FCFA 880M (US$1,446,000)!**

This sum can finance the total monthly municipal expenses across all 58 Divisions in Cameroon, with enough to finance another 18 such Divisions. In other words, the economic impact equals the total monthly budgets of 130% of Divisions in Cameroon whose combined population is 7 million working-age adults.

IN THE NORTHWEST

- 6X the 2017 budget for Justice
- 6.6X the 2017 budget for Vocational Training
- 2.4X the 2017 budget for Economic Planning
- 14X the 2017 budget for SME/Crafts Industries

Primary Education

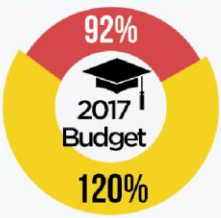


Secondary Education

IN THE SOUTHWEST

- 16x the 2017 budget for Justice
- 176x the 2017 budget for promoting Human Rights
- 2.8x the 2017 budget for Economic Planning
- 3.4x the 2017 budget for Vocational Training
- 4x the 2017 budget for SME/Crafts Industries

Secondary Education



Primary Education

Greater, two times over, than the total 2017 Public Investment Budget for Boyo Division

Greater, two times over, than ALL microfinance loans made in 2012 (benefitting 9,845 individuals and 464 CIG groups)

IN THE NORTH & SOUTHWEST

- 50x Public Investment Budget for Culture
- 4.6x Public Investment Budget for Justice
- 4.6x Public Investment Budget for Commerce

= combined monthly salaries of 24,262 minimum-wage employees + the total monthly salaries of 1,305 local elected officials, with enough left to pay 1,000 more

will pay for 102 public water boreholes

can build 96 classrooms

PARADIGM INITIATIVE

Source: @KathleenNdongmo

ParadigmHQ ParadigmHQ ParadigmHQ www.ParadigmHQ.org

Africa's Great Deficit In Internet Access As A Form Of Digital Rights Violation

The Internet's role in fostering individual and societal development is increasingly being recognized in national and international fora. This understanding was codified in goal 9 of the United Nations Sustainable Development Goals (SDGs)[19] which is to "build resilient infrastructure, promote sustainable industrialization and foster innovation". This goal acknowledged that "investments in infrastructure – transport, irrigation, energy and information and communication technology – are crucial to achieving sustainable development and empowering communities in many countries. It has long been recognized that growth in productivity and incomes, and improvements in health and education outcomes, require investment in infrastructure." The acknowledgment that ICTs, including the Internet, spur development is evident.

The United Nations Human Rights Council resolution in June 2016 also affirmed that Internet access is a human right. Furthermore, the June 2017 report of the *Special Rapporteur for the Promotion and Protection of the Right to Freedom of Opinion and Expression* to the Human Rights Council goes as far as saying that "the lack of adequate connectivity infrastructure, high costs of access imposed by government, gender inequality, and language barriers — that also may constitute forms of censorship"[20].

This is a valid and noteworthy point because while digital rights advocates draw attention to Internet disruptions, illegal surveillance and arrests of bloggers, they often ignore the crisis in the very poor investment in information and communications technology in Africa, which deprives millions of citizens access to the Internet. Internet penetration in Africa is 28.3%, almost half of the global average of 49.7%[21]. These statistics are the offshoot of the situation in countries such as Togo, Tanzania, Somalia, Sierra Leone, Niger, Mozambique, Malawi, Madagascar, Liberia, Guinea Bissau, Guinea, Chad, Eritrea, Congo Brazzaville, Democratic Republic of Congo, Comoros Islands, Central African Republic and Burundi, where despite having millions of citizens, Internet penetration is less than 10%.

This means that 9 out of 10 citizens of these African countries do not have Internet access. As suggested in the Special Rapporteur's report, when millions of citizens are denied access to connectivity due to deliberate government policies, this could be deemed censorship. There is research evidence for this type of activity[22], moreso for countries where government dominates the ICT sector, like Ethiopia where government operates a monopoly of telecommunications services.

[19] "UN Sustainable Development Goals: 17 Goals to Transform our World". http://bit.ly/1ONYpUu
[20] Amina Khan, "Ethnic groups' government influence and Internet access go hand in hand, study says". The Los Angeles Times, September 8, 2016. http://lat.ms/2cbX2oI
[21] "Internet World Stats". http://bit.ly/1f3mohY
[22] Nils BW, Suso B, Philipp H, Eduard G, Xenofontas D (2016). "Digital discrimination: Political bias in Internet service provision across ethnic groups". Science Vol. 353, Issue 6304, pp. 1151-1155. http://bit.ly/2yaiU00

The Human Angle:

Digital Rights Violations Affect Real Human Lives

It is sometimes the case that the millions of citizens across Africa for whom civil society groups advocate for their digital rights do not quite understand what it is all about. In countries where many live below the poverty line, advocating for digital rights sometimes seems like the occupation of the elite, with no bearing on the lives of ordinary people. In response to this, our Digital Rights in Africa report for 2017 places emphasis on the human stories behind digital rights abuses. We bring to the fore some of the incidents and stories from across Africa of ordinary people, representative of the average citizen across the continent, whose lives were disrupted and often endangered simply because they chose to exercise their rights online, or how individuals were made to suffer when their governments made the decision to disrupt Internet access. Through this commentary, we are saying to the millions of African citizens, when profiling the stories of victims of digital rights abuses in Africa: "this could be you".

We are not alone in this stance. The 9th point of the United Nations Human Rights Council (UNHCR) Resolution[23] of June 2016, states that the Council:

"Condemns unequivocally all human rights violations and abuses, such as torture, extrajudicial killings, enforced disappearances and arbitrary detention, expulsion, intimidation and harassment, as well as gender based violence, committed against persons for exercising their human rights and fundamental freedoms on the Internet, and calls on all States to ensure accountability in this regard;"

For the Internet to fulfil its developmental potential, African citizens from Cape Town to Cairo – all across the continent – must have the assurance that they can at least freely exercise online the same rights they enjoy offline.

[23] "The United Nations Human Rights Council (UNHCR) Resolution". A/HRC/32/L.20, June 27, 2017. http://bit.ly/2kqlMeN

Internet shutdown human profiles

A key gap in digital rights advocacy is the inability of civil society to present documentation of real human lives affected by digital rights violations such as Internet shutdowns. The following stories illustrate the scale of concern and missed – or nearly missed – opportunities which digital rights violations instigate.

The Google coding champion who almost never was

Nji Collins Gbah, 17, became the first African to win the prestigious annual Google coding challenge in 2017. The Google coding competition, open to pre-university students worldwide between the ages of 13 and 17 attracted more than 1,300 entries from young people from 62 countries[24].

To submit an appliscation, Collins had to complete 20 technically complex tasks assigned by Google from November 2016 to January 2017 using skills he learnt from online sources and books. As one of the 34 grand prize winners, Collins has the chance of visiting Google's headquarters and be inspired to do greater things. However, he almost missed this opportunity because just a day after the final deadline for submissions, the government deliberately cut off Internet connections in his home town of Bamenda. Collins only got to know of his award about two weeks into the Internet blackout. In order to continue learning and developing his coding skills, Collins had to travel about 370 km to Yaounde, Cameroon's capital city for access to the Internet.

In a different scenario, had the Internet blackout occurred a little earlier than it did, perhaps even affecting the whole country as is now fairly common in Africa, a great life-changing opportunity for personal development might have been lost by Collins, which is sadly the case for numerous other young people in Africa who are denied the opportunity to contribute towards the ailing economy of their countries.

[24] Abdi Latif Dahir, "Google's new coding champion is a 17-year-old Cameroonian whose hometown has been cut off the internet". Quartz Africa, February 14 2017. http://bit.ly/2gGNrYK

12 girls denied problem-solving opportunity

In a similar story, Sophie Ngassa, a teacher in Government Technical High School, Bamenda, Cameroon and a member of the Google Developer Group, could not successfully register 12 of her students for the 2017 Technovision Challenge because of the Internet shutdown in regions of the country. The Technovision Challenge[25] invites teams of girls around the world to solve local problems using technology skills. Although the girls have the opportunity of applying again next year, this year's application was an opportunity denied them by the action of their government. Besides, the girls may not be in a position to benefit from the opportunity next year, and this loss of opportunity might linger with them depending on how their futures pan out.

Worried parent cut off from vulnerable wards

The stories of Collins and Sophie illustrated above demonstrate an aspect of the negative impact Internet shutdowns have – the life-changing educational and developmental opportunities they shut the door on. During the Cameroonian Internet shutdown in January 2017, this narrative was perhaps best captured by the severe losses in income and opportunities incurred by Cameroon's budding tech industry, "Silicon Mountain", based mainly in the English speaking regions whose Internet connections were cut off. However, there were also stories of individuals whose losses and concerns during the Internet shutdown were of a more filial nature – the inability to keep in touch with vulnerable relatives in the region. A case in point is the story of a Cameroonian parent in the Netherlands who had 6 youngsters (her children and nieces) in Cameroon[26], and monitored their progress via internet. The Internet shutdown between January 17 and April 20, a period of 93 days, cut off all communication links with these vulnerable youngsters. She spoke of her concern particularly for the 4 girls amongst them, whom she feared might be lured into becoming young mothers, prematurely, as was the case of her other relatives. She narrated the psychological trauma occasioned by being unable to constantly be in touch, as any parent would want to.

[25] Technovision Iridescent. http://technovationchallenge.org/

[26] Nina Forgwe, "Cameroon's Internet Shutdown: The Human Factor". One Young World, April 6 2017. http://bit.ly/2xtrK53

2017 Digital Rights Violations Across Africa

This section of the report profiles 21 countries across the continent and features country demographics so that particular country contexts are clear. We also identified some of the Internet Service Providers (ISPs) working in each country because the digital rights environment in Africa is often influenced by these service providers, as the recent focus on the role of business in human rights demonstrates. Policies or laws that threaten Internet Freedom, and violations that have occurred so far in 2017, are also included for each country featured in this report. The Digital Rights in Africa Report of 2017 builds on the 2016 report to give a snapshot of some of the most important events in digital rights in Africa. The report methodology included desk research, all-year monitoring of digital rights across Africa and expert surveys of over 13 Country Researchers across Africa. Unless otherwise stated, country population data was obtained from the World Bank, while Internet penetration statistics obtained from the International Telecommunications Union (ITU), National Communications Authorities, Budde.com and InternetWorldStats.

The following countries, in respective regions of the continent, are featured in the report:

Central Africa: **Cameroon, Democratic Republic of Congo, The Republic of Congo.**
East Africa: **Ethiopia, Kenya, Somalia, South Sudan, Tanzania.**
North Africa: **Egypt, Morocco.**
Southern Africa: **Malawi, Namibia, Zambia, Zimbabwe**
West Africa: **Gambia, Liberia, Mali, Nigeria, Senegal, Sierra Leone, Togo**

Cameroon

Cameroon has a population of 23,439,190 and Internet penetration of 25%. ISPs in Cameroon include MTN, Nexttel (Viettel), Vodafone, Orange, CAMTEL and Yoomee (Wimax).

In Cameroon, there is no law that specifically addresses social media. However, Law N° 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime "governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon." This law, although applauded as a step towards containing the spreading menace of cybercrime, has been criticized for being light on digital rights and heavy on sanctions, particularly against freedom of expression. It contains two key sections that sanction online activity.

According to Section 77:

(i) Whoever uses electronic communication or an information system to act in contempt of race or religion shall be punished with prison terms from 2 years to 5 years or a fine of between 2 million to 5 million CFA francs or both.

(ii) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of stirring up hatred and contempt between citizens.

According to Section 78:

(i) Whoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest to its veracity or prove that the said piece of information was true shall be punished with a prison term of 6 months to 2 years or a fine of between 5 million and 10 million CFA francs or both.

(ii) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of disturbing public peace.

These sections were widely and repeatedly broadcasted through text messages to subscribers during the unprecedented 93-day Internet shutdown in the Northwest and Southwest regions of the country, from January 17 to April 20, 2017. This law effectively criminalizes online speech by holding criminally liable anyone who cannot "attest to the veracity" of information published or propagated online.

The 2010 Cybersecurity and Cybercrimes law fails to include sufficient protections against abuse of power and invasion of privacy, both of which can affect journalists and their sources online or offline. This law also holds

content and service providers along with social networks liable for content hosted on their servers. The overall result is a chilling effect on free speech because it creates a legal framework that can easily be used to silence dissent or to retaliate against those who publish unflattering reports about the government in power.

The Anti-Terrorism law of December 2014, on the suppression of acts of terrorism in Cameroon, was a welcome initiative in the fight against the Boko Haram terrorist organization in the Northern part of the country. However, its potential infringement on important human rights and freedoms protected under the Cameroon constitution and international human rights law was immediately revealed through the flood of criticisms that followed its promulgation. Many commentators echoed the fact that the vague definition of terrorism under the law could threaten freedom of expression, freedom of opinion, freedom of association and the freedom to take part in public protests.

A high-handed application of the anti-terrorism law will lead to disproportionate punishment for the exercise of civil rights and liberties, as witnessed when the Internet was shut down in Cameroon.

Similarly, the choice of the military tribunal as the only competent court for legal interpretation of the anti-terrorism law is also a cause for concern. The designation of military tribunals to try civilians contravenes the right to fair trial under the International Covenant on Civil and Political Rights. Military tribunals do not qualify as independent and impartial courts, as being part of the armed forces they fall under the executive branch of the government. Here again, the anti-terrorism law which carries disproportionate penalties for vaguely defined offences falls short of providing an opportunity for fair trial per international human rights standards.

Digital Rights Profile:

From January 17 to April 20 2017 – a 93 day period, the longest Internet shutdown in Africa was implemented in the English-speaking Northwest and Southwest regions of Cameroon. In response to political protests from its English speaking citizens calling for greater socio-political participation, the Internet shutdown followed mass arrests of citizens, particularly journalists and bloggers. This action by the Cameroonian government headlined digital rights violations in Africa in 2017 on account of its scale and impact.

Access Now, a civil society organization working for the defence of digital rights, estimated the cost of the 93-day Internet shutdown to the Cameroonian economy at $4.5 million[27]. An analysis of the first 30 days of the Internet shutdown in Cameroon revealed it cost $1,446,000 (or FCFA 880m), a sum large enough to finance the total monthly municipal expenses across all 58 municipal divisions in Cameroon, with enough spare to fund a further 18 such divisions. The challenges posed to the business community (particularly the tech industry) by the Internet shutdown are well documented[28]. However, while the economic costs of the Internet shutdown are well known, lesser known are the stories of human suffering and missed opportunities the Internet shutdown occasioned. Illustrated in the "Internet shutdown human profiles" section of this report, these stories show the intensely personal implications of an Internet shutdown to human development and welfare.

[27] "Victory in Cameroon: after 94 days, the internet is back on". AccessNow, April 20 2017. http://bit.ly/2fxMaUc
[28] Abdi Latif Dahir, "Reeling from an internet shutdown, startups in Cameroon have created an "internet refugee camp". Quartz Africa, March 28 2017. http://bit.ly/2hd0ZPF

A second Internet shutdown[29] was also reported in Cameroon in the wake of continued clashes between pro-independence protesters in Anglophone Cameroon and government forces. Government again ordered the Internet shutdown in the Anglophone regions of the country, while only social media sites were inaccessible in the rest of the country. MTN, the country's largest mobile operator, sent out text messages on the evening of October 1, saying it had problems with its internet connections[30]. Reports from Cameroon in November also indicate that Internet disruptions still persists in the country, particularly in the Anglophone regions of the country and many citizens are being forced to use Virtual Private Networks (VPNs).

[29] Julie Owono, "New Internet shutdown ordered in Cameroon". Internet Sans Frontieres, October 2 2017. http://bit.ly/2xcG2Xy
[30] "Cameroon internet shut for separatists". BBC News, October 2 2017. http://bbc.in/2xPMhT4

Democratic Republic of the Congo

With a population of 78,736,150 and Internet penetration of 6.21%, the Democratic Republic of Congo in recent years has emerged as one of the most important countries to watch for digital rights violations in the central African region. ISPs operating in the country include Société Congolais des Postes et des Télécommunications (SCPT), Orange Group and Bharti Airtel[31].

Act n° 013-2002 of 16 October 2002[32] is the primary legal instrument against digital rights in Congo DRC, and it confers on government powers to take over control of telecommunications facilities in the interest of national security or public defence. This legislation has been instrumental in implementing the Internet shutdowns in the country in recent years.

The Government has also commenced plans to update the Framework law 013-2002 on Telecommunications, as well as the e-Transactions Bill, and a law amending the Act that set up the regulator – the Authority of the Post and Telecommunications of Congo (ARPTC)[33]. The government plans to achieve this through a newly proposed Telecommunications and ICT bill, which has been drafted without public consultation and still retains much of the threats to digital rights such as granting the government right to interfere with communications and powers of surveillance.

Moreover, there are a number of laws, which activated, could be used to hurt the right to freedom of expression and digital rights in general. These include[34]:

Section 150 (h) of the Criminal code of 1940, which makes it an offence not to publish the full names and correct address of the author or publisher of any writing.

Sections 76 and 77 of the Press Freedom Act 96-002 of 1996 makes it "an offence to incite others (whether through speeches, writings, images or any other written means) to commit punishable offences, including theft, murder, looting, arson or any act threatening the stability of the state".

Section 77 of this Act also makes it an offence to publish anything that offends the President.

[31] BuddeComm, "Democratic Republic of Congo - Telecoms, Mobile and Broadband - Statistics and Analyses". http://bit.ly/2yvcjKa
[32] DLA Piper, "Telecommunications Laws of the World". Democratic Republic of Congo. http://bit.ly/2wY75uu
[33] "DR Congo Parliament Urged to Pass Laws That Support Citizens' Rights Online". CIPESA, June 15 2017. http://bit.ly/2hApwyc
[34] Justine Limpitlaw, "Media Law Handbook for Southern Africa, Volume 2", Democratic Republic of Congo: Konrad Adenauer Stiftung. http://bit.ly/2xMQgBO

It is also important to state that the provisions of the Constitution which covers freedom of expression (such as freedom of expression and access to information) are very problematic, in that these provisions contain internal limitations such as compliance with certain unstated public statutory provisions, public morals and order.

Digital Rights Profile:

In August 2017, authorities in the Democratic Republic of Congo mandated telecommunications companies to slow down Internet bandwidth to restrict the public's ability to upload pictures through social media[35]. This followed the refusal of the President to step down after expiration of his mandate in December 2016, when an Internet disruption was also implemented in the country. As was the case in Cameroon, this meant the Democratic Republic of Congo implemented two Internet disruptions within the space of a few months, demonstrating the increasing boldness of the government to use Internet shutdowns to stifle dissent. Government's willingness to implement drastic acts of censorship such as Internet shutdowns is sometimes a signal of a weak civil society. In this regard, the central African region has emerged as a country where civil society intervention needs strengthening. In the past two years there has been 7 separate incidents of Internet disruptions in 5 countries in the region – the highest in Africa and a worrying trend.

[35] "Congo orders internet slowdown to restrict social media: telecoms source". Reuters, August 7 2017. http://reut.rs/2xlyM9o

Republic of the Congo

The Republic of Congo has a population of 5,125,820 and Internet penetration of 8.12%. ISPs operating within the country include Alink Telecom, Congo Telecom, MTN Congo, AMC Telecom, Offis, Azur-Wifly, Airtel Congo, Mobi.

Digital Rights Profile:

On June 11, as the country approached legislative elections and amid protests by the opposition, Internet access to the Republic of Congo was lost. The official explanation given by government was that a fishing vessel offshore cut the country's link to the continental cable system. This stance, doubted by a section of the public, was corroborated by MTN Congo and several government sponsored media[36]. The doubt expressed in some quarters of Congolese society concerning the origin of the Internet disruption is not unfounded. The fact of the disruption happening in the midst of opposition protests in the country raised suspicions, given that the government successfully implemented a disruption of telecommunications services around the elections of March 2016. However, Internet connection was restored within two weeks[37].

[36] Brett L. Carter, "Something is happening in Congo-Brazzaville". African Arguments, June 20, 2017. http://bit.ly/2iEXt0H
[37] Ismail Akwei, "Internet connection restored in Congo-Brazzaville after 15 days". Africanews, June 27, 2017. http://bit.ly/2iE3St4

Egypt

With a population of 95,688,680 and Internet penetration of 39.21%, Egypt has one of the highest populations of Internet users in Africa. The numerous ISPs operating in Egypt include Etisalat Misr, Nile online (EG), TE Data, Vodafone and Link Egypt.

Digital rights in Egypt has been largely influenced by the turbulent politics of the country in the past few years. Digital rights have borne the brunt of the current military government's bid to hold on to power by all means and prevent democracy from gaining a foothold in the country. Legislation and policies in Egypt which violate digital rights often show the hand of government against Internet freedom. The 2015 Counter-Terrorism law, for instance, has often been used to silence government critics. Article 29 of the law allows sentencing of up to 10 years in prison for creating a social media account that promotes "terrorist" activities or "harms national interests"[38]. Also, under the Telecommunication Regulation law, Internet Service Providers must give full access to all the equipment and software needed for the Armed Forces and national security agencies to exercise their power, in a clear breach of rights to privacy[39].

Online journalists have in particular paid a heavy price for their free reportage of the tense political situation in Egypt, making the country one of the most dangerous places for journalists in Africa.

The events that would shape the digital rights scene in Egypt for 2017 began in earnest in December 2016, when Egyptian authorities censored access to the encrypted messaging app, Signal[40], with many users in the country unable to use the service. In response, on December 21, 2016, Open Whisper Systems updated the Android version of the app, which includes anti-censorship techniques for users likely to be based in Egypt.

In April, it emerged that 60 members of the Egyptian parliament approved a social media draft law[41], which if approved, would allow authorities to have Egyptian citizens register their details with the government in order to access social media sites such as Facebook and Twitter. The draft law also stipulates a 6 month prison term and a fine for dissenters.

[38] "Egypt: 10-year prison term for insulting president an outrageous assault on freedom of expression". Amnesty International, April 13 2017. http://bit.ly/2xjEKeM
[39] Marwa Morgan, "How surveillance, trolls, and fear of arrest affect Egypt's journalists". Committee to Protect Journalists, June 12 2017. http://bit.ly/2xxmDnU
[40] Joseph Cox, "Signal Claims Egypt Is Blocking Access to Encrypted Messaging App". Motherboard, December 19 2016. http://bit.ly/2xx4oPs
[41] Afef Abrougui, "Draft Law Would Require Egyptian Social Media Users to Register With Government". Advox Global Voices, May 5 2017. http://bit.ly/2w9zl34

Digital Rights Profile:

On April 12, an Alexandria court sentenced lawyer Mohamed Ramadan to 10 years in prison[42], five years under house arrest and a five-year ban on using the Internet. For a Facebook post criticizing the President, he was convicted on charges including insulting the President, misusing social media platforms and incitement to violence under the counter-terrorism law, demonstrating the danger posed by the law to freedom of expression in Egypt.

In 2017, the Egyptian government implemented one of Africa's most comprehensive censorship and surveillance programmes. This includes the blocking of at least 21 websites[43] which included major news sites, blocking access to the Tor network[44] (which citizens used for anonymous browsing) and the extensive surveillance of online journalists[45], which led to a climate of fear and self-censorship within the ranks of bloggers and online journalists.

[42] "Egypt: 10-year prison term for insulting President an outrageous assault on freedom of expression". Amnesty International, April 13 2017. http://bit.ly/2kJXLnZ
[43] Ahmed Aboulenein, "Egypt blocks 21 websites for 'terrorism' and 'fake news". Reuters, May 24 2017. http://reut.rs/2yL3Fs
[44] Maria Xynou, Vasilis Ververis, Arturo Filastò and Wafa Ben Hassine. "#EgyptCensors: Evidence of recent censorship events in Egypt". Open Observatory for Network Interference (OONI), June 19 2017.http://bit.ly/2gogmof
[45] Marwa Morgan, "How surveillance, trolls, and fear of arrest affect Egypt's journalists". Committee to Protect Journalists, June 12 2017. http://bit.ly/2xxmDnU

Ethiopia

Ethiopia has a population of 102,403,200 and Internet penetration of 15.37%. Ethiopia is unique in Africa for having a very powerful state-owned monopoly over telecommunications and Internet services through Ethio Telecom. Legislation typically used to impinge on digital rights include the Telecom Fraud Offence Proclamation, the Computer Crime Proclamation and the anti-terrorism law.

Digital Rights Profile:

Ethiopia's leadership on the continent on the use of Internet shutdowns is well reported. In 2016, Twitter and WhatsApp services were shut down in the Oromia region of Ethiopia in response to protests by citizens seeking greater socio-political inclusion within the country, and also in a bid to prevent the leakage of examination questions for 10th and 12th grade students.

Ethiopia continued the trend of Internet shutdowns in 2017 with Internet disruptions reported during the national school leaving examinations for over 1 million high school students[46]. The Ethiopian Internet shutdown was confirmed from publicly available data sources on Internet network disruptions such as Ripe Atlas, which reflected a drop in Internet traffic from Ethiopia.

In 2017, numerous Ethiopian citizens were arrested for comments made online. These include opposition politician Yonatan Tesfaye who was on May 25 given a six-year prison sentence after being found guilty of "encouraging terrorism" for comments he made on Facebook[47]. His sentence for comments made in criticism of the government's use of excessive force on the Oromia region protesters demonstrates how Ethiopia's anti-terrorism law has been used to stifle freedom of expression in the country.

Similarly in May, Getachew Shiferaw, the former editor-in-chief of opposition newspaper, Negere Ethiopia, was sentenced to one year and six months in prison for making what the government considered "inciting comments" in a private message he sent to his colleagues on the Facebook messenger app[48]. In reality, the so called inciting comments were really criticism of the government

[46] "Ethiopia imposes 100% internet blackout to protect integrity of exams". Africanews, May 31 2017 http://bit.ly/2x15tMZ
[47] "Ethiopian politician jailed for six years for Facebook comments". BBC News, May 25 2017. http://bbc.in/2vVJLZD
[48] "Ethiopian Protester Sentenced to Six Years Behind Bars for Facebook Posts". Advox Global Voices, May 26 2017. http://bit.ly/2wrPypk

Also in Ethiopia, the Supreme Court on April 6, 2017 decided that two members of the Zone 9 bloggers, who blog about human rights, good governance and social justice in the country, and who had been acquitted of terrorism charges, should instead face charges for inciting violence through their writing. If convicted, they face a maximum sentence of 10 years[49].

Artists too have come under the heavy government clampdown in Ethiopia on freedom of expression. In June, Seena Solomon, a rising musical talent in Ethiopia, was arrested together with her producers and performers for uploading 'resistance music' on YouTube[50]. Seena, being a member of the Oromia ethnic group in Ethiopia, had used her music to lend credence to the yearnings of her community for greater inclusion in Ethiopia – an act which the government categorized as incitement. This follows the arrest of Temeri Mekonen, another popular musician, also for incitement through music. The arrest of musicians for YouTube posts in Ethiopia is just another reflection of the stifling environment around freedom of expression in the country.

Ethiopia is one of the most restrictive states in Africa for freedom of expression and digital rights. The government has a long history of mass surveillance of citizens and arrests of critics. This brings to the fore the fact that these profiles shared only reflect some of the cases which came to public knowledge. The impunity within government to perpetuate digital rights violations like Internet shutdowns is reflected in a quote attributed to Dr. Debretsion Gebremichael, Ethiopia's Minister of Information Communications Technology Development, when speaking with Horn Affairs, an online news agency covering the Horn of Africa region, during the May 2017 Internet shutdown in Ethiopia. Dr. Gebremichael, whose portfolio includes overseeing Ethio-telecom, the state owned monopoly, was quoted as saying:

> ***"You don't need a monopoly to shut down the Internet, you only need to be a government."***

Few will argue against the fact that Ethiopia is perhaps the most repressive environments for digital rights in Africa, and ought to be a focus point for more intense civil society effort.

[49] "Ethiopia Supreme Court says two Zone 9 bloggers should face incitement charges". Committee to Protect Journalists, April 6 2017. http://bit.ly/2vVRvuC
[50] "Ethiopian Musicians Charged With Terrorism for 'Inciting' Song Lyrics". Advox Global Voices, July 14 2017. http://bit.ly/2xn6otm

Gambia, The

The Gambia has a population of 3,719,300 and Internet penetration of 18.5%. ISPs operating in The Gambia include Gamtel, QuantumNet, Netpage, and Airtip. The 1997 constitution guarantees freedom of speech and press freedom, though fundamental freedoms were severely restricted under former President Yahya Jammeh, who was defeated at the December 2016 polls by the incumbent Adama Barrow.

Over the years the Jammeh-led government successfully amended existing legislation to increase penalties for certain offenses. In some cases draconian laws were enacted to further undermine freedom of expression and media freedom. The criminal code, which had already criminalized defamation with a minimum prison sentence of one year plus heavy fines, was amended in April 2013 to penalize individuals for "giving false information to public servants" with up to five years in prison. Analysts believe the amendments were part of efforts to intimidate citizens, journalists and potential whistle-blowers from seeking legal recourse for the abuses they often experience at the hands of the authorities.

A legislation specifically targeting Information and Communication Technologies was passed in July 2013 in the form of amendments to the 2009 Information and Communication Act. Under the new amendments, online dissent is specifically criminalized with penalties of up to 15 years in prison, fines of up to GMD 3 million (about US$100,000), or both, for using the internet to criticize, impersonate, or spread false news about public officials[51].

The telecommunications sector is regulated under The Gambia Public Utilities Regulatory Authority Act 2001, which established the Public Utilities Regulatory Authority (PURA) in 2004 to regulate the activities of telecommunication service providers and other public utilities.

[51] "Freedom on the Net Report 2015". Freedom House, Washington DC.

Digital Rights Profile:

Arrests and prosecutions of online journalists and ICT users for expressions using ICTs formed part of a common feature in The Gambia for many years although it is hoped that the democratic transition in the country will see digital rights improve.

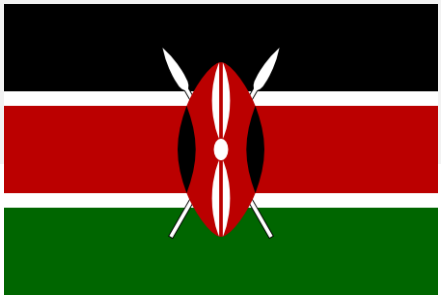
Following President Jammeh's rejection of the election results of December 2016, the hashtag #GambiaHasDecided[52] began to trend on Gambian and regional blog sphere. A civil movement emerged from the hashtag organizing activities, printing t-shirts and erecting billboards. During the five weeks (9 December - 21January) of political impasse some members of civil society were forced to flee the country, following death threats. Despite the hostile environment under Jammeh, Gambian activists (online and offline) stood their ground and rendered great services to their country men and women.

Between the months of July and August 2017, a group soldiers were arrested and detained[53] for allegedly running a WhatsApp group with messages inimical to national security. The soldiers were also accused of loyalty to the former president (Yahya Jammeh) and trying to destabilize the country. They remain in detention without charges.

In late October 2017, the hashtag #OccupyWestField started trending as activists planned a peaceful protest at the head office of the National Water and Electricity company (NAWEC). The hashtag generated huge interest as the populace grappled with acute power cuts and water shortages. As per local requirements, mobilizers behind the hashtag sought police permit for the peaceful protest. Unfortunately, the office of the Inspector General of Police (IGP) denied the request and deployed anti-riot police on the site of the planned protest.

From the WhatsApp group arrests to the #OccupyWestField permit denial, there is genuine suspicion that the new administration intends to use the repressive laws promulgated by President Jammeh. Overall, there is a renewed sense of hope for improved civil liberties in the Gambia, although recent actions of the incumbent government are a source of concern.

[52] Muhammed Lamin Saidykhan, "#GambiaHasDecided: Reflections on a dramatic transition". Pambazuka News, May 11 2017. http://bit.ly/2yGAF4h
[53] Mustapha Darboe, Gambia: "Four soldiers arrested for suspected mutiny". Smbc News, July 19 2017. http://bit.ly/2ALydLt



Kenya

Kenya has a population of 48,461,570 and Internet penetration of 26%. Safaricom, Airtel, Telkom Kenya, Finserve Africa, Zuku, Liquid Telecom and Jamii Telcom are some of ISPs operating in the East African country.

With 2017 being an election year in Kenya, the National Cohesion and Integration Act which stipulates penalties for hate speech came into the spotlight as a legal route through which freedom of expression online could be proscribed in the country. Also, Article 24 of the Kenyan constitution provides conditions for limiting rights and fundamental freedoms and Article 36 of the National Intelligence Services Act limits the right to privacy in the constitution (in Article 31) where there is suspicion of an act of terrorism.

Digital Rights Profile:

Early in the year, the Communications Authority of Kenya sought powers to monitor calls and text messages of Kenyans[54]. In a related move which clearly showed the hand of a government preparing for the August 2017 elections, the authorities announced that they had purchased surveillance equipment worth a total of $9.3 million to monitor social media and mobile phones, and that the Internet might be shut down in the event of election violence[55].

Although these measures were ostensibly taken to prevent a reoccurrence of the election violence during the 2007 elections in the country when over a thousand people lost their lives and hundreds of thousands were displaced, the absence of clear legal safeguards to protect citizens' privacy made these measures a threat to digital rights. Policies taken by the Kenyan government to safeguard the elections also include announcing plans to restrict political commentary[56], in a move that critics observed could limit freedom of expression and active citizen participation during elections.

When Facebook announced plans to launch an educational tool in English and Swahili to limit the spread of fake news and hate speech on its site[57], the move raised concerns that the government could take advantage of what they would tag inappropriate use of social media during the elections. During and after elections on August 8, 2017, and the repeat elections on October 26, Kenyan authorities followed the example of Nigeria in 2015 and Ghana in 2016 by not shutting down the Internet, demonstrating that Internet shutdowns in Africa during elections and political processes should not be a default position. It is hoped that the Internet is left on and digital rights are respected in Kenya as the political situation in the country unfolds.

[54] Edwin Okoth, "Big Brother could start tapping your calls, texts from next week". Daily Nation, February 17 2017. http://bit.ly/2eZLDdb
[55] "Kenya may 'block internet' during elections". BBC News January 13 2017. http://bbc.in/2jEVY3o
[56] "Kenya seeks to restrict political commentary on social media ahead of elections", July 5, 2017. http://bit.ly/2xrqenF
[57] Abdi Latif Dahir, "Facebook has joined the battle to combat fake news in Kenya". Quartz Africa, August 2 2017. http://bit.ly/2x8fbzL

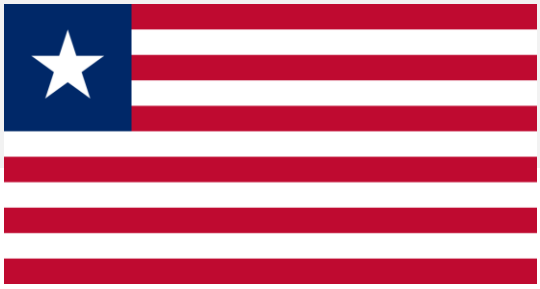
Considerable progress was made during the year in the defence of digital rights. In a landmark decision, a Kenyan court declared section 194 of the country's penal code, which creates the offence of criminal defamation and had been used to restrict online freedom of expression in the country, illegal[58]. There was also a legal challenge to the government's plans for surveillance of citizens, with a court temporarily putting on hold the plans[59].

Also, and perhaps setting a new trend, two Whatsapp administrators were arrested around elections in August for allegedly sharing hate messages[60] and fake news[61]. Japheth Mulewa and Langton Jamil were both arrested in separate incidents for sharing hate speech and fake news respectively.

There were also arrests of citizens for posts and comments made online. Barely into the start of the year on January 14, Seth Mutugi, a staffer in the communications department of Meru county was arrested for a defamatory Facebook message[62] posted on January 6 about the Meru County executive for Sports, Gender, Youth and Social Services, Joy Karui. The post had alleged impropriety in the bidding for the contract for Kinoru stadium. Blogger Robert Alai was on August 18, 2017, arrested for a story featuring pictures of members of Kenya's first family[63] in a hospital that he published on his Facebook page. Blogger Elijah Kinyanjui was joined in a case of defamation by Hon. John Mututho for a Whatsapp post[64] alleging inappropriate financial dealings, which Mr Mututho denied.

Although there were no disruptions of Internet connectivity in Kenya during the August 8 and October 26 elections, the political atmosphere in the east African country was tense when a court invalidated the election results which saw the incumbent Uhuru Kenyatta returned as President. Furthermore, on October 10, the opposition candidate Raila Odinga withdrew from the election rerun, explaining that the necessary reforms to guarantee a credible election have not been implemented.

[58] "Kenya: Court strikes down criminal defamation laws". Article 19 Press release, February 6, 2017. http://bit.ly/2yiUGOt
[59] Mohammed Yusuf, "Kenya Court Upholds Suspension of Mobile Phone Monitoring". Voice of America (Africa), March 6, 2017. http://bit.ly/2jCAKTy
[60] Alphonce Gari, "WhatsApp group administrator held for allegedly spreading hate messages". The Star, August 17, 2017. http://bit.ly/2w2zT05
[61] Ismail Akwei, "Kenyan man detained over post-election hate messages on WhatsApp". http://bit.ly/2f5ECHM
[62] Shitemi Khamadi, "Meru County official Seth Mutugi arrested for defamation over Facebook post". #iFreeKenya, January 15 2017. http://bit.ly/2xMsQgH
[63] "Blogger robert alai arrested after leaking photos of kenyattas in hospital", Nairobinews, August 19 2017. http://bit.ly/2xbyKrb
[64] Shitemi Khamadi, "John Mututho seeks legal action against Safaricom, WhatsApp, Google for defamation". #iFreeKenya, August 17 2017. http://bit.ly/2wtLEBh



Liberia

Liberia has a population of 4,613,820 and Internet penetration of 7.32%. ISPs in Liberia include the state owned LibTelCo (formerly Liberia Telecommunication Corporation), Lone Star, Orange Liberia and Nova Phone.

Digital Rights Profile:

While there are no incidents of digital rights violations to be reported for Liberia, the country attained a milestone in digital rights that has been difficult to reach in most of Africa in 2017. This milestone pertains to the proposed decriminalization of press offenses, particularly libel, which is one of the most widely used legal avenues for stifling freedom of expression in Africa.

To this effect, on July 20, 2017, Liberia's President, Ellen Johnson Sirleaf, submitted to the national parliament a bill titled "An Act to Amend the Liberian Codes Revised, Penal Law of 1978[65]". This bill was scheduled to be signed before Liberia's general elections in October 2017, and it is hoped that the decriminalization of libel within Liberia will lead to an environment where freedom of expression is respected, in actual practice. It is also hoped that this bold move in Liberia will lead to more progressive changes in legislation across Africa, where press laws have been typically used to gag the press and limit freedom of expression online.

However, reports from Liberia[66] suggest that the bill has not been passed into law as planned. Liberians have expressed fears that the inauguration of a new government might lead to the abandonment of this bill and a revert to the status quo in the country. The bill represents a bright spark in digital rights and we hope that the incoming government completes the process of its passage into law.

[65] "Major Boost for Free Expression as President Sirleaf Submits Anti-Criminal Libel Bill to Parliament". Media Foundation for West Africa, August 4 2017. http://bit.ly/2hk7ekP

[66] Abednego Davis, "Liberia: Rep. Dunah 'Not Sure of Decriminalizing Anti-Free Speech Bill Passage'". Daily Observer, September 28 2017. http://bit.ly/2zG1N7N

Malawi

Malawi has a population of 18, 298, 679 and an Internet penetration rate of 9.61%. There are 50 licensed Internet service providers in Malawi and 6 licensed telecommunications operators, namely, Malawi Telecommunications Limited, Telekom Networks Malawi Limited, Airtel Malawi, Access Communications, Lacell, and Celcom.

Digital Rights Profile:

Although Malawi has registered isolated incidents of digital rights violations, in 2016 the Malawi Parliament passed two pieces of legislation, the Communications Act 2016 and the Electronic Transactions Act 2016, which may infringe on citizens' rights of privacy and free expression. The two pieces of legislation came into force on 1st June 2017.[67]

The Communications Act provides for the regulation of the provision of services in the electronic communications sector and information society in Malawi.[68] Part XI of the Act comprising sections 92 through 94 provides for mandatory registration of generic numbers and SIM cards. Section 92(1) provides:

"A person who uses a generic number or owns or intends to use a SIM card for voice telephony services shall register that generic number or SIM card with any electronic communications licensee or with the distributor, agent or dealer of the electronic communications licensee, authorized to provide or sell generic numbers or SIM cards."[69]

Network operators or their agents are required to register generic numbers and SIM cards by obtaining and filling, in a form, the following information: the full name of the subscriber; the identity card number, or any other document that proves the identity of the subscriber; and the residential and business or registered physical address of the subscriber. For potential subscribers that are legal entities, network operators must obtain particulars of the subscriber, together with a certified copy of the subscriber's certificate of registration or incorporation; business licence; and where applicable, taxpayer identification certificate number. Network operators may also obtain from the potential subscriber any other information that they deem necessary.[70]

Before filling in the particulars of a potential subscriber referred to above, a network operator must verify the information and retain certified copies of the documents obtained.[71] Use of an unregistered generic number or SIM card is a criminal offence punishable by a fine and imprisonment for two years.[72] The Malawi Communications Regulatory Authority confirmed[73] that mandatory SIM card registration started in June 2017 as

[67] Malawi Government Gazette
[68] Communications Act. 2016, Long Title.
[69] Communications Act, 2016, section 92(1)
[70] Communications Act, 2016, section 92(2)
[71] Communications Act, 2016, section 92(3)
[72] Communications Act, 2016, section 94
[73] Interview with Daniel Chiwoni, Director of Legal Services, Malawi Communications Regulatory Authority.

reported in the media.[74] According to the Malawian Government, one of the justifications for mandatory SIM card registration is stated to be combating crime.[75] However, there has not been any conclusive evidence showing that that SIM card registration helps to reduce crime.[76] On the other hand, African SIM registration requirements appear to be part of a growing trend on the continent toward government monitoring and control of the communications infrastructure.[77] As observed by Frank La Rue, the *UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression*, SIM registration facilitates the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location tracking, and simplifying communications surveillance. Such SIM users' information can be shared with Government departments and matched with other private and public databases, enabling the State to create comprehensive profiles of individual citizens.[78]

Writing about privacy in Africa, Steve Song pointed out that with an International mobile subscriber identity-catcher (IMSI catcher), it is possible for state agencies to listen passively to mobile phone traffic and pick up the identity of all of the phones in a given area which can then be matched with data on the SIM card registration database to identify people participating in an anti-government protest in a given area,[79] thereby enabling governments to identify and target political opposition.[80] In the absence of solid data protection legislation, SIM card registration may therefore seriously threaten citizens' rights to privacy and to express themselves freely.

Part XIX of the Communications Act deals with electronic monitoring and enforcement. Section 167 thereof gives the Malawi Communications Regulatory Authority (MACRA) the power to use an electronic monitoring system to monitor and enforce licensees' compliance with the Communications Act. It provides as follows:

"The Authority shall use the appropriate technology to establish, install, and maintain an electronic monitoring system to monitor the activities of licensees to ensure and enforce compliance with this Act and licences issued by the Authority: Provided that a system shall not be used for monitoring actual content of communication, network traffic or for any other purpose other than for its monitoring mandate under this Act."[81]

Where the establishment of the electronic monitoring system requires connection with a licensee's network, the licensee is required to provide appropriate interface sites between the electronic monitoring system and its network to ensure direct submission of data to the monitoring system.[82]

Thus, broadly speaking, the Communications Act allows monitoring of the activities of network operators as opposed to those of subscribers. However, there is no clear delimitation in the provision of exactly what constitutes activities of network operators that should be monitored. Suffice to say that at the time the Act came into force, MACRA had already acquired electronic monitoring technology known as Consolidated ICT Regulatory

[74] Nyasa Times, "*Dausi says Malawi starts mandatory sim card registration*". *Nyasa Times,* 11 July 2017, http://bit.ly/2gvdt1n
[75] Maravi Post, "*Mandatory sim card registration silently starts in Malawi*". Maravi Post, 11 July 2017, http://bit.ly/2xXjoaS
[76] K. Donovan and A. Martin, "The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change", [2014] 19(2-3) *First Monday* available at http://bit.ly/2zHellD
[77] *ibid*
[78] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (UN Human Rights Council, 17 April 2013), UN Doc A/HRC/23/40 at p 19
[79] Steve Song, 35 Reasons to worry about privacy in Africa, (*Many Possibilities*, 17 September 2012) available at http://bit.ly/2yZR6MS
[80] Privacy International, Zimbabwe threatening privacy rights with new SIM registration database, (2 October 2013) available at http://bit.ly/2yJuPSC
[81] Communications Act 2016, section 167
[82] Communications Act 2016, section 168

Management System (CIRMS) whose capabilities include: quality of service monitoring, fraud prevention, revenue monitoring, equipment identity monitoring, interception of voice, audio, internet and short messages (SMS), spectrum management, and global satellite linkage facilitation.[83]

Two Malawian citizens challenged MACRA's decision to acquire CIRMS.[84] In justifying its decision to acquire CIRMS, MACRA's Director General swore an affidavit stating that the purpose of CIRMS was to enable MACRA monitor the activities of network operators in real time to ensure: (i) the accuracy of traffic information and therefore the revenue generated; (ii) compliance to the quality of service standards; (iii) checking and removal of illegal traffic; and (iv) control fraud which affects revenue generated and levels of licence fees due.[85]

However, the Malawi Supreme Court of Appeal acknowledged that the deployment of CIRMS presented a serious threat to citizens' rights to privacy, access to information and free expression stating that:

"What comes to the fore therefore, is that both parties agree that the machine in question is indeed capable of a wide range of functions. It is capable of intercepting various forms of communications as we stated earlier. We should acknowledge that the amount of information that can be made available from any of the various functions of the machine can in turn be used for a plethora of purposes. These limitless possibilities of use of the machine makes it a potentially dangerous and volatile equipment. There is no denying that potentially dangerous equipment in the wrong hands becomes lethal. We want to acknowledge further that any power that is capable of being abused will eventually be abused."[86]

The Supreme Court further acknowledged the concern that CIRMS could actually be used to eavesdrop on private conversations and that the mere existence of such surveillance programs had a chilling effect on citizens' rights to free expression. The court weighed these concerns against the regulatory objectives of the Communications Act 1998, namely, consumer protection, revenue monitoring and quality of service monitoring which would be better met using CIRMS. Subject to an undertaking made by MACRA that it would not use the monitoring system to intercept private communications, the Malawi Supreme Court of Appeal allowed MACRA to deploy CIRMS.

The Communications Act also prohibits use of the electronic monitoring system for monitoring actual content of communication or network traffic.[87] However, this does not diminish the serious threats to citizens' fundamental rights to privacy and freedom of expression posed by CIRMS. Since section 167 of the Communications Act prohibits monitoring of actual communications content, it can be safely assumed that instead it allows monitoring of metadata, that is, information about the actual communications content, such as its origin, destination, time, frequency, etc. Through monitoring of metadata, it is possible to draw precise conclusions concerning the private lives of persons whose communications data has been accessed and retained over time.[88] Such data may also make it possible to create a log of what a person has been accessing online,[89] which grossly violates citizens' rights to privacy and free expression.

---

[83] The Malawi Government Gazette, 3rd April 2009
[84] *Malawi Communications Regulatory Authority v Hophmally Makande and Eric Sabwera* (Malawi Supreme Court of Appeal, Civil Appeal Case Number 28 of 2013)
[85] *Ibid*
[86] *ibid* at page 25
[87] Communications Act 2016, section 167
[88] *Digital Rights Ireland Ltd v Ireland, and Kärntner Landesregierung Michael Seitlinger, Christof Tschohl and others v Austria,* Joined Cases C-293/12 and C-594/12 at para [27] available at http://bit.ly/1yF25p3
[89] Graham Smith, 'An Itemised Phone Bill Like None Ever' (Cybereagle, 16 January 2016) available at http://bit.ly/2ittWYi

Furthermore, as David Kaye has pointed out, direct access by the authorities to Internet and telecommunications networks, as is the case under the scheme of the Communications Act 2016, would enable authorities to intercept and monitor communications with limited legal scrutiny or accountability.[90] The Malawi Communications Regulatory Authority (MACRA) is now in the process of deploying Consolidated ICT Regulatory Management System (CIRMS).

Section 24 (1) of the Electronic Transactions Act (ETA) 2016 declares that 'Subject to this Act, there shall be no limitations to online public communication.' Subsection (2) allows restriction of online public communication on somewhat broad and vague grounds such as to 'protect public order and national security' and to 'facilitate technical restriction to conditional access to online communication'.[91] The provisions' breadth and vagueness could be open to abuse and result in unjustified restriction of internet access and negatively affect end users' fundamental rights.[92] The provisions do not satisfy the legality requirement for limitation of fundamental rights and are thus open to challenge.[93]

Authorities can use data gathered through the electronic monitoring system to determine which websites to block. In the light of the broad and vague provisions allowing restriction of Internet access under the ETA 2016, there is a real threat that this may be used by repressive regimes to suppress dissent.

[90] David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Human Rights Council, 30 March 2017, UN Doc A/HRC/35/22 at p 8 para 22

[91] Electronic Transactions Act, 2016, section 24(2)

[92] Freedom House, Freedom On The Net 2016: Malawi at p 7, available at http://bit.ly/2xddTjH

[93] *Sunday Times v UK* [1979] ECHR 1 at paragraph 49 where the court stated: *'Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct...'*; see also David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN HRC, A/HRC/35/22) 30 March 2017 at page 5 para 10 emphasizing that: *'Internet shutdowns ordered pursuant to vaguely formulated laws and regulations ... fail to satisfy the legality requirement.'*

Mali

Mali has a population of 17,994,840 and Internet penetration of 11.11%. ISPs in Mali include Sotelma, Afribone Mali SA, Orange Mali SA and Ikatel SA.

Digital Rights Profile:

In June, protests greeted the Malian government's attempt at constitutional amendment which was widely viewed as an attempt to give the President more powers. In response to these protests, the government shut down access to Facebook and Twitter[94] in the west African country, a repeat of the shutdown of Facebook in 2016. Malians were forced to use Virtual Private Networks (VPNs) to access these websites, demonstrating the growing knowledge of circumvention tools among Malians.

The news that Malians took up the use of VPNs should be encouraging to civil society working on digital rights in the region, because this knowledgeable reaction from a section of the Malian public is not always replicated across Africa during Internet disruptions. Like we noted in our 2016 report, when governments face informed and unified responses to digital rights violations like Internet shutdowns, there will be hesitation in their determination to continue down that path.

Madou Kante, a popular blogger known for his incisive socio-political commentary and criticism of social ills in Mali, escaped an assassination attempt on June 19 2017[95]. Through his blog, Madou Kal Journal, there are suggestions that he had upset powerful interests in the country, especially as constitutional amendments to give more powers to the President were underway.

[94] Julie Owono, "Internet Sans Frontières Calls on the Government of Mali to Keep the Internet On". Internet Sans Frontieres, June 19 2017. http://bit.ly/2xKBQCc
[95] "Blogger Survives Assassination Attempt". Media Foundation for West Africa, July 31 2017. http://bit.ly/2k1mN1Q

Morocco

Morocco has a population of 35,276,790 and Internet penetration of 58.27%. ISPs operating in the country include Maroc Telecom, Meditel and Inwi.

Article 218 – 6 of Morocco's anti-terrorism law gives the government legal powers to filter and delete content that is deemed to "disrupt public order by intimidation, force, violence, fear or terror". This legislation has been used as a pretext to detain online journalists and bloggers. The penal code articles criminalizes the defamation of state institutions, "causing harm" to Islam, glorifying terrorism and "inciting against territorial integrity". These offences are broadly defined, and can be used by authorities to implicate free speech[96]. Although the recent Press and Communications Law adopted in 2016 makes a number of advances in reforms governing speech, it still maintains most of the speech offenses of its predecessor – the 2002 Press Code[97].

Digital Rights Profile:

Following mass protests in the town of Al-Hoceima of the Rif region in Northern Morocco triggered by the death of a fish monger[98] occasioned by local law enforcement officials, authorities slowed down Internet connections and also shut down Internet access in order to control the spread of the protest.

In the wake of the protest, numerous arrests of online journalists and bloggers who covered the events were made. These arrests were violations of their rights. Some of those arrested include:

i. (i) Hamid El Mahdaoui, the editor of the Badil.info news website, was arrested on 20 July[99] while filming the protest and charged in court.

ii. (ii) Ahmed Rachid, a photographer and cameraman with the Lakome2 news website, was also beaten while filming police dispersing demonstrators during the protests[100].

iii. (iii) Mohammed Al-Asrihi, the director of the opposition news website Rif24, was arrested on June 6, 2017. He had produced video coverage of the protests in the Rif area of northern Morocco, and of its imprisoned leader Nasser al-Zefzafi for the website[101].

[96] "Morocco: Scrap Prison Terms for Nonviolent Speech". Human Rights Watch, May 4, 2017. http://bit.ly/2xv7vUL
[97] "The Red Lines Stay Red": Morocco's reforms of its speech laws. Human Rights Watch, May 4, 2017. http://bit.ly/2xflBt2
[98] "Morocco protests: Activist Nasser Zefzafi arrested". BBC News, May 29 2017. http://bbc.in/2w733fk
[99] "Morocco obstructs coverage of Rif protests". Reporters without borders, July 23, 2017. http://bit.ly/2wqQEp8
[100] Ibid
[101] "Moroccan website director held in solitary confinement pending trial". Committee to Protect Journalists, June 16, 2017. http://bit.ly/2viqWiV

In an unrelated incident in July[102], a court in Rabat gave sentences under the terrorism charge, ranging between one and two years, to eight members of the youth wing of the Justice and Development Party. The group made Facebook posts praising the assassination of the Russian ambassador to Turkey by a police officer in Turkey in December 2016. They had been arrested in late December 2016. While the actions of these young men might not be excused, it is clear that the Moroccan authorities violated their rights by treating them as criminals and terrorists.

[102] "Eight Moroccans Given 1-2 Years in Prison for Praising Assassination of Russian Ambassador", Morocco world news, July 15, 2017. http://bit.ly/2viDRS4

Namibia

Namibia has a population of 2,479,710 and Internet penetration of 31%. ISPs operating in Namibia include Telecom Namibia, MWeb, Africaonline, MTC, ITN, Verizon and Paratus Telecom.

ADigital Rights Profile:

Legislation which can be exploited to hurt digital rights include the drafted Electronic Transaction and CyberCrime Bill which permits unauthorised access to communications, warrant-less surveillance and interception. The draft bill has no provisions for personal data and privacy protection.

The Namibian government, in June 2017, released a social media policy which although well intentioned, might have the effect of fostering self-censorship and limit freedom of expression. The Social Media Use Policy[103] tabled in the National Assembly by information minister Tjekero Tweya outlined guidelines for government officials' use of social media accounts in an official capacity and also advised on its use outside of official hours. In the wake of the policy's launch, there have been concerns expressed about the possibility of civil servants implementing self-censorship in order to protect their careers.

In March 2017, the Communications Regulatory Authority of Namibia (CRAN) had announced enforcements for SIM Registrations[104] following a consumer appeal by MTC, a service provider, to have its subscribers go through a registration process. This process was however halted partly because Part 6 of Chapter V (5) of the Communications Act which sets out the legal provisions for the registration of SIM cards had not been implemented. As with any of SIM registrations, data protection and privacy is a major concern.

[103] Shinovene Immanuel, "Govt warns on social media posts". The Namibian, June 14 2017. http://bit.ly/2f5zuDc
[104] "SIM registration process halted", The Namibian Sun, April 12 2017. http://bit.ly/2havCoZ

Nigeria

With a population of 185,989,640 and Internet population of 47.7%, Nigeria has the largest number of Internet users in Africa. ISPs operating within the country include MTN, Globacom, Airtel, MainOne, Swift, Spectranet, Smile and 9Mobile.

There are numerous laws and policies which impinge on digital rights in Nigeria. However, in recent years, Nigeria's Cybercrime law, particularly sections 24 and 38 have been the principal legal instrument for stifling freedom of expression in the country. This legislation has been used to instigate the arrest of citizens and journalists for comments made online, as the profiles below show. Also, set against the background of the secessionist Biafra movement in south east Nigeria, where ethnic and sectarian exchanges have been aired on social media channels, steps have been taken by the Federal government to control social media in the country. The Terrorism Amendment Act (the amendment to Terrorism Prevention Act of 2011) scaled second reading in November 2016[105], and is being viewed in some quarters as a route to stopping ethnic sentiments online, which the Federal government now likens to terrorism.

A bill to repeal and re-enact the Cybercrime Act of 2015 is before Nigeria's parliament because its content and exact purpose is unclear, digital rights groups are closely watching the development.

Similarly, and following the same trend, it has emerged that a draft executive bill on hate speech has been submitted to the Ministry of Justice[106]. Although intended to check toxic ethnic and religious exchanges on platforms such as social media, there are fears it might also be used to proscribe freedom of expression. These fears are not unfounded, because the Nigerian military recently announced that they have commenced the monitoring of social media[107] for inciting comments bordering on hate speech which threaten the unity of the country. The National Council on Information, at the end of an extraordinary meeting on "Hate Speeches, Fake News and National Unity" held on Friday July 21, 2017, in Jos, Nigeria, recommended the setting up of a Council to regulate the use of social media in Nigeria[108].

In a move which also clearly demonstrates government's increasing powers of surveillance, the Federal government announced the planned launch of two communications satellites[109] with capability for mass surveillance of citizens. In Nigeria's largest city and commercial capital, Lagos, the government also announced the review of legislation granting oversight over print and online publications[110], stating the government's determination to register media houses in the state. These plans have stoked fears of censorship and regulation among civil society, fears that have been allayed by the Commissioner of Information and Strategy, who

[105] Samuel Ogundipe, "Bill to strengthen Nigeria's anti-terrorism law scales second reading". Premium Times, November 15 2016. http://bit.ly/2hpzl1T
[106] Wale Akinola, "Hate speech will soon become criminal offence in Nigeria". Naij.com, http://bit.ly/2jZdNua
[107] "We Now Monitor Social Media For Anti-Government And Anti-Military Information – Military". Channels Television, August 23, 2017. http://bit.ly/2yAYlY8
[108] "Nigeria Plans Council to Regulate Social Media Use". Nigeria Communications Week, July 24 2017. http://bit.ly/2wfrrL6
[109] "CSO Raises Alarm, Sues FG for Spying on Nigerians with Satellites". Nigeria Communications Week, June 20 2017. http://bit.ly/2jWRBAL
[110] Gbenga Salau, "Ambode to regulate newspapers, magazines, online media". The Guardian, May 30 2017. http://bit.ly/2xFt4Fk

explained that these steps have not been conceived with any negative intention by the state government. It also emerged in June that the sponsored surveillance of citizens' communications by a number of state governments in Nigeria discovered and reported[111] in 2015 has continued unabated.

On January 20, 2017, a High Court ruled against Paradigm Initiative, Media Rights Agenda and Enough is Enough Nigeria in their joint bid to challenge the constitutionality of sections 24 and 38 of Nigeria's Cybercrime Act which has been the main legal instrument for the arrest of citizens and online journalists. The court ruled that the two sections of the Cybercrime law are not unconstitutional. However, an appeal has been lodged at the Appeal Court, with no date set at yet for the case to be heard. Also, it emerged that using section 146 of the National Communications Act of 2003, the government has surreptitiously commenced moves to take down website and blogs which the government deems offensive, under the guise of national security[112]. There are fears this latest action by the government could also be expanded to regular users of social media and online forums, given reports that millions of Nigerian's mobile phones of Nigerians in the Federal capital have been bugged by security agencies[113].

Digital Rights Profile:

In 2017, many citizens, bloggers and online journalists were punished for comments made online. On January 2, a Journalist with Ibom Nation newspaper in Uyo, Mr Jerry Edoho was arrested by the police for sharing[114] a post on Facebook alleging a plane crash by one of Nigeria's airlines. On January 19, the offices of Premium Times, an influential news website, was raided[115] by the Nigerian Police after defamation complaints from legal representatives of the Chief of Army staff. Both the publisher and the Judiciary correspondent were arrested and a search of the premises was conducted without a warrant. Mr Aku Obidinma, a radio broadcaster[116], after 60 days in detention for Facebook posts criticizing the Imo state government, was finally released on January 17, 2017. He was arrested on November 21, 2016.

On February 17, Audu Maikori, a popular businessman, was arrested for tweets he posted on the Southern Kaduna killings in Northern Nigeria[117]. He had withdrawn and apologised for false claims in his tweets, stating that he was misled by his source. However, in October, a Federal High Court in Abuja ordered the Governor of Kaduna state and the police to pay Mr Maikori the sum of 40 million naira as compensation for his illegal arrest[118]. This court order does not however preclude his ongoing trial in Kaduna. Mr Austin Okai was on April 9 arrested in Abuja for his social media posts deemed unacceptable to the Kogi State government[119]. On April 19, Midat Joseph, Bureau Chief of the Leadership Newspapers in Kaduna State was arrested for alleged incitement on a Whatsapp group[120] that called for protests against the killing of civilians. In March, police in Ibadan arrested Kemi Olunloyo, a popular blogger for an Instagram post[121] making allegations of infidelity against a Nigerian

[111] Samuel Ogundipe, "INVESTIGATION: Two years after, Niger Delta states continue controversial spying programmes". Premium Times, June 30 2017. http://bit.ly/2fLqZxT
[112] Dare Adekanbi, "FG clamps down on online newspapers, others". Nigerian Tribune Online, November 5, 2017 http://bit.ly/2ztO7cY
[113] Nicholas Uwerunonye, "DSS Bugs 70% Of Mobile Phones In Abuja", Independent, November 8 2017. http://bit.ly/2zrkCuV
[114] Eric Dumo, "Police arrest, fly journalist to Abuja over Facebook post". Punch Newspapers, January 7 2017. http://bit.ly/2ynKZxK
[115] "January in West Africa: New Dawn in Gambia, Massive Police Crackdown in Nigeria, Media Bans Lifted in Benin". Media Foundation for West Africa, February 7 2017. http://bit.ly/2fLV7t4
[116] "Imo State Deputy Gov. Got Me Detained For 60 Days Over Facebook Post - Radio Broadcaster". Sahara reporters, July 4 2017. http://bit.ly/2fM6Wj4
[117] Samuel Ogundipe, "Police arrest Audu Maikori, Chocolate City boss". Premium Times, February 17 2017. http://bit.ly/2youbqd
[118] Jayne Augoye, "Federal High Court Orders El-Rufai, Police, To Pay Audu Maikori N40 million Over Illegal Arrest". Sahara Reporters, October 28 2017.
[119] "Arrest of Austin Okai: Impunity taken too far – Group". Nigerian Vanguard, April 9 2017. http://bit.ly/2jV1miE
[120] Ameh Comrade Godwin, "Police releases Leadership journalist arrested in Kaduna". Daily Post Nigeria, April 22 2017. http://bit.ly/2ynP0SQ
[121] "Police Arrest Kemi Olunloyo Over Blog Post Accusing Pastor Of Adultery". Sahara Reporters, March 17 2017. http://bit.ly/2fLVzHL

pastor. On June 2, Charles Otu, a correspondent with Guardian Newspaper, was assaulted in Abakaliki for Facebook comments critical of the Ebonyi state government[122].

On June 10, Frank Utoo was arrested in Abuja for comments made on Facebook[123] which was deemed insulting by a prominent political leader in Kogi state. On June 15, Danjuma Katsina, a journalist, was arrested in Katsina over comments questioning the legitimacy of a newly elected member of Nigeria's House of Representatives from the state[124]. In March, Gambo Saeed was sentenced to nine months imprisonment by a Chief Magistrate court for defaming the governor of Katsina state in northwest Nigeria[125]. On August 3, Johnson Musa was arrested by State Security Service operatives for posting an image of the state governor's Abuja residence in a Whatsapp post[126], alongside comments which were deemed inappropriate by the authorities. A primary school teacher, Biodun Baba, was arraigned before a magistrate court in Ilorin on July 27 for allegedly insulting Senate President Bukola Saraki on Facebook[127]. The charges against him were however withdrawn[128].

The large number of people, including journalists, arrested by security agencies in Nigeria for comments made online in 2017 is troubling, and presents urgent work for civil society towards ensuring that the right to freedom of expression is respected in the country.

[122] Nnamdi Akpa, "Journalist beaten to stupor over Facebook post". The Guardian, June 5 2017. http://bit.ly/2wOegVJ
[123] Yemi Itodo, "Social activist, Franc Utoo abducted in Abuja". Daily Post, June 10 2017. http://bit.ly/2wOxcE0
[124] Abdulaziz Abdulaziz, "Police detain Nigerian journalist over Facebook post". Premium Times, July 16 2017. http://bit.ly/2fLY6lu
[125] "Man jailed for insulting, defaming Nigerian governor on social media". Premium Times, March 27 2017. http://bit.ly/2xFuTST
[126] Johnson Aluko, "Youth docked for exposing Bello's Abuja residence". The Guardian, August 5 2017. http://bit.ly/2xFKFgw
[127] Success Nwogu, "Civil servant arraigned for anti-Saraki Facebook posts". The Punch Newspaper, July 28 2017. http://bit.ly/2wRsL6D
[128] Nnenna Ibeh, "UPDATED: Charges against Kwara civil servant who criticized Saraki withdrawn". Naij.com http://bit.ly/2xwvT9E

Senegal

Senegal has a population of 15,411,610 and an Internet penetration of 22.66%. ISPs operating in the country include Orange, Expresso, Tigo and Arc Informatique.

The Code of Criminal Procedure (Sections 90-10 and 90-14) and Criminal Code (sections 254, 255 and 258) have been used by the authorities to stifle freedom of expression in the country. Although Senegal's new press code contains provisions which enhance freedom of expression, new clauses recently introduced further erode whatever gains might have been achieved[129]. Articles 224 and 225, for instance, impose stiffer fines and prison terms for press offences. Article 28 of the revised draft electronic communications code of the Ministry of Posts and Telecommunications of Senegal has clauses which threatens the principle of net neutrality and opens the door for government oversight of traffic management, surveillance and the potential blocking of services. Civil society in Senegal have expressed reservations about this legislation[130].

Digital Rights Profile:

Four young Senegalese citizens in their twenties, three women and one man, were imprisoned on Friday June 2, 2017, for posting a doctored photograph of the President in a Whatsapp group[131]. Amongst them is Ouleye Mané, who works for the local Touba TV. Bassirou Sakho, the legal counsel to one of the women, narrated that they were charged with sharing an offensive image and criminal conspiracy. In Senegal, punishment in the for sending offensive images ranges from one month to two years imprisonment with fines ranging from 25,000 to 300,000 CFA.

In a similar incident, a famous Senegalese artist, Amy Colle Dieng, was arrested on August 3 for being the originator of an audio recording, that was widely circulated on Whatsapp,[132] and was deemed insulting to the President. The administrator of the Whatsapp group through which the recording was circulated, Amadou Seck, was also arrested. The arrest of Amadou follows the example of Kenya[133], where two administrators of Whatsapp groups were arrested on account of posts from users.

[129] "Senegal's New Press code: A step forward, two steps backwards", Media Foundation for West Africa, July 12, 2017. http://bit.ly/2xqUzjL
[130] Ndiaga Gueye, "The Ministry of Posts and Telecommunications of Senegal legalizes the censorship of the Internet, our freedoms threatened". ASUTIC Senegal, June 30 2017. http://bit.ly/2iP1n3Y
[131] "President's Cartoon: Senegalese Journalist Freed from Six Weeks' Detention". Media Foundation for West Africa, August 16, 2017. http://bit.ly/2xriuj4
[132] "Case Amy Collé Dieng: the administrator of the WhatsApp group stopped by the DIC". August 7, 2017. http://osiris.sn/Affaire-Amy-Colle-Dieng-I.html
[133] "WhatsApp: Why you'd think twice becoming admin", Daily Nation, August 19, 2017. http://bit.ly/2iCMfKk

There were also reports that there were severe disruptions to Internet and telephone services in Sédhiou (a region in southern Senegal) for about four months[134], mainly affecting subscribers of the Orange Telephone company operating in the region.

[134] Yanne Evelyne, "Senegal: Orange network of Sédhiou disrupted for 4 months". Africa Telecom and Technology Review, July 3, 2017. http://bit.ly/2vIlajH

Sierra Leone

Sierra Leone has a population of 7,396,190 and Internet penetration of 11.77%. ISPs operating in the country include Airtel, Africell, AFCOM, Smart, Sierratel, Onlime and Diakem.

The Public Order Act of 1965 criminalizes the publication of materials with the intent to incite the public. However this legislation is vaguely worded and has been abused to imprison journalists and activists over the years in Sierra Leone. Proposed changes to the 1991 national constitution includes a new chapter in the 1991 Constitution on "Information, Communication, and the Media".

The chapter on Information, communication, and the media seeks "to bring about an independent media[135]." Although this chapter guarantees the freedom and independence of the media, it excludes protection for the following types of speech, which are not defined, leaving room for interpretation at the discretion of the government: propaganda for war, incitement to violence, hate speech, or advocacy of hatred.

The Constitution Amendment Committee also recommended the establishment of an 11-member media regulatory body.

Digital Rights Profile:

The government of Sierra Leone launched a massive nationwide campaign to educate citizens against the "misuse" of social media. The Information Minister explained that at least 24,000 people will be deployed across the country to assist this effort, geared towards easing tensions as the country approaches elections in February 2018. In a threat that bodes ill for digital rights in the country, the Minister made it clear that should this "last-ditch" effort fail, the government will clamp down on social media in the country through "stringent laws"[136].

Similarly, the Sierra Leone government, through Momoh Konteh, the Chairman of the National Telecommunications Company announced that they had signed an agreement with the management of Facebook for the monitoring of derogatory materials online[137]. Although many citizens of Sierra Leone doubt the veracity of the government's claim, it has been rightly criticized by civil society and other active citizens as an attempt to instil fear amongst citizens towards curbing their free use of social media.

[135] Library of Congress Global Legal Monitor. http://bit.ly/2vuHVht
[136] Philip O, "Campaign against social media abuse rolled out in Sierra Leone". http://bit.ly/2wamHHn
[137] Alhaji Koroma, "NATCOM Threatens Control of Social Media". Salone Today, July 24, 2017. http://bit.ly/2gbthcQ

On July 26, 2017, Francis Josiah appeared in court on six charges of defamatory libel[138] for an "offensive" Whatsapp post against the Minister of Information's family and was granted 100 million leones ($13,000) bail in August 2017. While Francis' posting of the Minister's family pictures on a Whatsapp group, "Monologue/D Good Governance," and criticizing their lifestyle amid claims of corruption, was deemed distasteful by some, this action did not warrant a criminal prosecution.

[138] Sylvia Villa, "Sierra Leone News: WhatsApp posts offend MIC". Awoko, July 27 2017. http://bit.ly/2xil7U0

Somalia

Somalia has a population of 14,318,000 and Internet penetration of 1.88%. Internet Service Providers present in the country include Telesom, Somtel, Nationlink, Hormuud, Netco and Golis telecom.

The Somali cabinet on July 13, 2017 approved draft revisions to the country's media laws with far reaching consequences for freedom of expression. Under this legislation, penalties of up to US$1,500 will be imposed on those convicted of fake news[139]. This clause, which does not clearly define what constitutes fake news, could be used to stifle freedom of expression and press freedoms. Also, the Parliament in July 2017 began considering a draft National Communications Bill aimed at setting a legal and regulatory framework for the telecoms sector. The legislation is also designed to curb burgeoning cybercrime in the country[140].

Digital Rights Profile:

Abdirahman Arab Da'ud, a journalist with the Hangool news website was arrested on April 11, 2017 for an online news article critical of Somaliland's (autonomous region of Somalia) Police Commissioner[141]. Similarly, Ahmed Ali Kilwe, an online Journalist was detained on July 2, 2017 by the counterterrorism police in Puntland (an autonomous region of Somalia) for a Facebook post criticizing the Puntland President's use of public funds[142]. Ahmed Omar Saeed, a journalist with Horseed media, was arrested on August 6, 2017 for his Facebook post which alleged that the President of the Puntland autonomous region of Somalia, Abdiweli Mohamed, operated a counterfeit money printing outfit[143]. There were also reports that the Somaliland government blocked access to 5 websites including Karinnews, Baraarugnews, Saylactoday, Haleelnews and Suradnews[144]. In a related incident, Internet companies in Somaliland blocked access to websites critical of their interests[145].

Following the examples of countries such as Gambia and Uganda, it has been reported that the Somaliland electoral body had plans in place to shut down Internet access during elections commencing November 13 and ending November 17 2017[146] to prevent the spread of fake news and inciting comments online. This plan, although condemned by local and international actors who point to the examples of nations such as Nigeria and Ghana who held successful elections without blocking Internet access, was carried out as access to social media was blocked during the elections.

[139] Muthoki Mumo, "Q&A: Somali editor says efforts to make media law less restrictive don't go far enough". Committee to Protect Journalists, August 2, 2017. http://bit.ly/2wCljiR
[140] "Somalia: Parliament Passes Communication Act aiming to Regulate the Telecom Industry and Contain Cyber Crimes". Horn Observer, August 9 2017. http://bit.ly/2gCHa0o
[141] "Somaliland journalist detained over critical coverage of police". Committee to Protect Journalists, April 11, 2017. http://bit.ly/2gBwoat
[142] "Puntland journalist jailed after criticizing president". Committee to Protect Journalists, July 7, 2017. http://bit.ly/2iZm5Sf
[143] "Journalist detained without charge in Puntland". Committee to Protect Journalists", August 9, 2017. http://bit.ly/2x7ChXP
[144] Khadar Nouh, http://bit.ly/2eYN9wv
[145] Judy Maina, "Somaliland internet firms block access to news sites, raising censorship spectre". AllEastAfrica, January 5, 2017, http://bit.ly/2iXbpTS
[146] "Somaliland to shut down the Internet during elections". Garowe Online, November 7 2017. http://bit.ly/2iPZ0OA

South Sudan

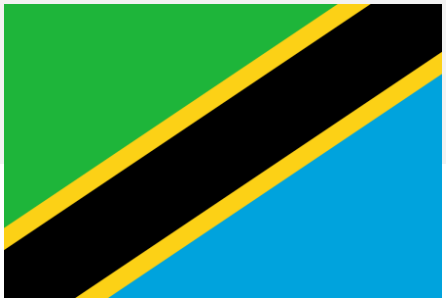
According to National Bureau of Statistics of South Sudan, the country has a population of 13,096,190 people. Its internet penetration is 20.5% according to National Communication Authority and some of the country's internet service providers are Zain, MTN and Vivacell.

South Sudan does not have specially crafted Internet laws, bills or policies. However, the government has had ICT policies in place since 2012, only for setting up government structures, as one of the requirements for the Northern Corridor Integration Projects of countries in the East African region. Also, as demonstrated this year, the National Communications Authority, an agency of the Ministry of Information, Communication and Postal Services, has the authority to block websites deemed offensive to the government.

Digital Rights Profile:

In July, South Sudanese authorities, through the National Communications Authority, blocked four news websites and blogs critical of the regime[147]. The websites of Radio Tamazuj and Sudan Tribune news were reportedly blocked and were inaccessible to many Internet users. Also, the popular Paanluel Wel and Nyamilepedia blogs for the Neur and Dinka tribes were also blocked and inaccessible. Although the government announced these measures were taken because these sites published subversive material, there are indications they were taken down for being critical of the regime. South Sudan is currently in the midst of a civil war, with factions fighting for control of the country.

[147] "SOUTH SUDAN: Authorities Block Access to at Least four Media Websites". Somali news, July 21, 2017. http://bit.ly/2x4sEbw



Tanzania

With a population of around 57 million, Tanzania has an internet penetration rate of around 13%. ISPs operating in Tanzania include AfricaOnline, Afsat Comm. (T) Ltd., Alink (T) Ltd., Benson Informatics Ltd. (BOL), Cats-Net, Costech, Satcom Networks, SimbaNet, Star Tel (T) Ltd, Tanzania Telecommunications Company Limited, University Computing Centre, Vizada Network, Vodacom (T) Ltd, WiA Co. Ltd, Zee Communications Ltd, Zanzibar Telecom Ltd.-Zantel, Selcom Broadband Ltd.[148]

Digital Rights Profile:

Tanzania has in the recent years been rocked by an unprecedented human rights crisis as evidenced by government's gross violations of citizens' freedom of expression rights through the passing of laws that are being used to silence any form of criticism or dissent.[149] In their Joint Situation Note, The International Federation for Human Rights (FIDH) and the Legal and Human Rights Centre (LHRC) state that between 2016 and 2017 alone, Tanzania has banned at least eight media houses; arbitrarily arrested and detained at least 27 journalists; and arrested 32 ordinary citizens some of whom have been charged for having publicly or privately criticized the President or his government.[150]

In September 2017, the Tanzania Communications Regulatory Authority opened a public consultation on the Draft Electronic and Postal Communications (Online Content) Regulations, 2017. The Regulations will come into force once signed by Tanzania's Minister of Information, Culture, Arts and Sports.[151] According to Tanzanian authorities, the Regulations are aimed at curbing moral decadence online and protecting national security and strengthening social and political cohesion in Tanzania.[152] The Regulations will apply to all online content including application services, bloggers, internet cafes, online content hosts, online forums, online radio or television, social media, subscribers and users of online content, and any other related online content.[153]

Part III of the Regulations sets out general obligations for online content. Online content providers will be required to 'ensure that online content is safe, secure and does not contravene the provisions of any written law'. They will further be required to 'use moderating tools to filter prohibited content' and 'put in place mechanisms to identify source of content'.[154] Additionally, online content providers will be required to remove prohibited content within 12 hours of being notified. Subscribers and users of online content will be responsible and

[148] Tanzania Internet Service Providers Association (TISPA), List of current Members, (2017) http://bit.ly/2iJqRje
[149] FIDH and Legal and Human Rights Centre, "Tanzania: Freedom of Expression in Peril- A Joint Situation Note, 1 August 2017, http://bit.ly/2iPQrTA
[150] *ibid*
[151] "Government tightens noose on social media", *The Citizen*, 25 September 2017, http://bit.ly/2zAq6B1
[152] *ibid*
[153] Draft Electronic and Postal Communications (Online Content) Regulations, 2017, Reg. 2.
[154] Reg 5(1)

accountable for information they post in online forums, social media, blog and any other related media.[155] Online content providers will be obliged to cooperate with law enforcement officers in pursuing functions under the Regulations.[156]

Application services licensees will be required to incorporate into their terms and conditions of service the right to deny access or terminate service where a subscriber contravenes the Regulations and to remove prohibited content.[157] Bloggers and online forums will be required to register with the Tanzania Communications Regulatory Authority and where the blog or online forum allows the general public to post content, they will be required to set mechanisms that content will not be published prior to the blogger's review. Additionally, bloggers will be required to use moderating tools to filter content and set mechanism to identify the source of such content.[158] These requirements shall apply to Tanzania residents, Tanzanian citizens outside the country, non-citizens of Tanzania residing in the country, blogging or running online forums with contents for consumption by Tanzanians.[159]

Internet cafes shall be required to put in place mechanisms to filter access to prohibited content and to install surveillance cameras to record and archive activities inside the cafe.[160] Regulation 10 emphasizes that every social media user shall be responsible and accountable for the information he publishes on a social media.[161] What constitutes prohibited content is set out in Regulation 12 in very broad terms as including indecent content, obscene content, hate speech, pornography, content that threatens national security, false content that is likely to mislead or deceive the public except where such content is clearly pre-stated to be parody, satire, or fiction. Hate speech includes defamatory material.[162] Contravention of the provisions of the Regulations will attract a fine of not less than five million Tanzanian Shillings or imprisonment for a term of not less than twelve (12) months or both.[163]

The Regulations do not meet the international human rights standards for the protection of the right to freedom of expression online. As has been pointed out by the Media Council of Tanzania, the Draft Regulations overly restrict media freedom and freedom of expression in general through unnecessary censorship, prohibition of anonymity, requirement for registration of bloggers and online forums, wide scope of prohibited content, and the giving of intermediaries power to interfere with citizens freedom of expression.[164]

[155] Reg 5(2)
[156] Reg 5(3)
[157] Reg 6
[158] Reg 7(1)
[159] Reg 7(2)
[160] Reg 9
[161] Reg 10
[162] Reg 12
[163] Reg 16
[164] Media Council of Tanzania, "Online Content Regulation will strangle freedom of expression", *The Guardian,* 4 October 2017, http://bit.ly/2hx050V

For instance, what constitutes prohibited content is capable of multiple interpretations and manipulation and could thus be used by government to determine what content should be accessed online thereby undermining editorial independence.[165] Again, mandatory registration of bloggers and online media could be deemed to be tactical censorship which may be used to restrain press freedom.[166] In addition, the requirement that bloggers and online forums set up mechanisms for the identification of their sources of content could dissuade individuals from providing information for fear that their identity may be disclosed.[167]

[165] *ibid*
[166] *ibid*
[167] *ibid*

Togo

Togo has a population of 7,606,370 and Internet penetration of 11.31%. ISPs operating in Togo include Togo Telecom, IMET, CAFE, BIB and IDS.

Digital Rights Profile:

In September, Togo joined the growing list of African nations to implement Internet shutdowns in response to political protests by citizens. Internet and telecommunications services in Togo were disrupted between Tuesday, September 5, 2017, and Sunday, September 10, 2017. Internet access in the country was also disrupted on September 19 with access to social media and mobile messaging blocked. These disruptions were the government's response to citizens' protests demanding for democratic change in the country, after decades of political leadership of Togo vested in one family. As with any Internet disruption, there were reports of the suffering[168] caused by this prolonged disruption in Togo. Access Now, a digital rights organization, also calculated that the first Internet shutdown (September 5 - 10) in Togo cost the country's economy a minimum of $1.8m, excluding mobile money, the informal sector and disrupted supply chains. This translates to a sum of $300,000 per day in a country with GDP per capita of $578.

In response to the Togolese Internet disruption, a coalition of over 30 organizations led by Paradigm Initiative wrote a protest letter to the ECOWAS Commission, African Union, African Commission for Human and Peoples' Rights, African Court for Human and Peoples' Rights and the United Nations Human Rights Council.

The Togolese government's recourse to an Internet disruption to quell protests is probably borne out of similar examples which they have observed across the continent.

[168] "Dispatches from an internet shutdown — Togo". AccessNow, 22 September 2017. http://bit.ly/2y6CuLq

Zambia

Zambia has a population of 16,591,390 and Internet penetration of 25.51%. Internet Service Providers operating within the country include Microlink Solution, CEC Liquid Telecommunications, Zamtel, Iconnect Zambia, Vodafone, CopperNet Solutions, Hai Telecommunications, Paratus Telecom, ZamNET, A Plus Technologies, IWAY Zambia, Preworx Zambia, VSAT Communication Ltd and Massnet Innovation Solutions.

Zambia, like much of Africa, has sections in its penal code which implicates freedom of expression through criminal libel, particularly through section 191 of Chapter 87 Penal Code and Section 59 of Cap 87 of the Laws of Zambia which criminalizes defamation of the President.

Digital Rights Profile:

In demonstration of the potency of criminal libel in Zambia, on Thursday, April 14, 2017, Chilufya Tayali was arrested and charged with criminal libel against the constitutional office of the Inspector General of Police, General Kakoma Kanganja[169]. In a Facebook post, Tayali accused Mr. Kanganja of "covering up for his inefficiencies when he charged and arrested United Party for National Development (UPND) leader, Hakainde Hichilema with treason".

In a related case, Patriotic Front Deputy Secretary General Mumbi Phiri sued Asher Hakantu for posting defamatory words on a Whatsapp group[170] between May 6 and May 8, where he alleged Mumbi Phiri came to political prominence through sacrificing her son, who in fact had died alongside other students in a case of wilful negligence on the part of the police and school authorities. Similarly, Edward Makayi was arrested for defamatory remarks[171] against the President and other state officials on a Facebook page under the name of Royson Edwards M, contrary to section 59 of Cap 87 of the Laws of Zambia which prohibits defamation of the President. This case in particular showed a renewed cooperation between the Zambian police and the Zambian ICT Authority – a cooperation which could have implications for digital rights in the country.

[169] "Chilufya Tayali Arrested and charged with criminal libel". Lusaka Times, April 14 2017. http://bit.ly/2hcRpbZ
[170] Mukosha Funga, "Social Media Hurts – Mumbi Phiri". News Diggers, July 20 2017. http://bit.ly/2xakRqp
[171] "Police arrest engineering student for 'insulting' President Lungu on Facebook", Lusaka Times, July 25 2017. http://bit.ly/2y9122a

Zimbabwe

Zimbabwe has a population of 16,529,904[172] and an internet penetration rate of about 50%.[173] Zimbabwe's ICT market comprises 16 licensed internet service providers that are registered with the Zimbabwe Internet Service Providers Association (ZISPA). These include: Africom Zimbabwe, Afrihost, Aptics, Clay Bytes Solutions, Econet Wireless, FBNet, Frampol, Liquid Telecom, Powertel, SADACNET, Telco, Telecel, Utande, YoAfrica, ZARnet, and ZOL Zimbabwe.[174] There are also five licensed telecommunication operators, namely, TelOne, NetOne, Telecel, Econet and Africom.

The Cybercrime and Cybersecurity Bill, 2017, generated a heated debate about the protection of digital rights in Zimbabwe. Initially introduced by government in 2013 as Computer Crimes and Cyber Crimes Bill 2013, the Bill was aimed at curbing cybercrime. However, commentators argued that the Bill is aimed at tightening government's grip over the control of cyberspace and spy on its citizens, and that it thereby infringed on basic people's rights such as freedom of expression and privacy.[175] After a series of public consultations, government is expected to table the Bill in Parliament before the end of 2017.[176]

According to its Long Title, the purpose of the Bill is, among others, 'to provide for and to consolidate cyber-related offences with due regard to the Declaration of Rights under the Constitution and the public and national interest…' While the recognition of protection of fundamental rights by the Bill should be lauded, the Bill's most unsettling provision is section 17 which criminalizes the transmission of false data message intending to cause harm. Section 17 of the Bill provides that *'any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intent to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment*'.

It has been rightly pointed out[177] that section 17 of the Bill attempts to bring back the controversial offence relating to publication of falsehoods under Section 31 of the Criminal Law Codification and Reform Act which the Supreme Court of Zimbabwe declared to be unconstitutional due to its chilling effect on the right to free expression.[178] Further, section 17 of the Bill bears some close resemblance with criminal defamation provisions in Section 96 of the Code, which again were declared unconstitutional by the Supreme Court of Zimbabwe in

[172] United Nations, Department of Economic and Social Affairs, Population Division, World Population Prospects: The 2017 Revision (2017), http://bit.ly/2cXsyqX
[173] According to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) internet penetration rate in the second quarter of 2017 was 48.6% having dropped from 49% in the first quarter: POTRAZ, Abridged Postal and Telecommunications Sector Report 2nd Quarter 2017 at p 17, http://bit.ly/2hX5IBE; POTRAZ, Abridged Postal and Telecommunications Sector Report 1st Quarter 2017 at p 14, http://bit.ly/2xXYtUW
[174] ZISPA Members, http://bit.ly/2yBzkiE
[175] Zimbabwe Independent, Cyber Crimes Bill: Its Flaws, remedies, 13 January 2017, http://bit.ly/2jNXMpT
[176] ITWeb Africa, Zimbabwe Finalises new cybercrime bill, 29 August 2017, http://bit.ly/2xdfeqJ
[177] MISA Zimbabwe, *Audit of Cybercrimes and Cyber Security Bill 2017,* 14 September 2017, http://bit.ly/2f9bRNI
[178] *The State v Chimakure, Kahiya & ZimInd Publishers (Pvt) Ltd* Constitutional Application No. SC 247/09

February 2016.[179] Thus section 17 of the draft Cyber Crimes and Security Bill 2017 would similarly have a chilling effect on freedom of expression online. It would most specifically affect social media which a majority of the citizenry in Zimbabwe has embraced as a means of communication and mobilization online.

The draft Cyber Crimes and Cyber Security Bill 2017 is a clear manifestation of the Zimbabwe Government's efforts to tighten its grip on cyber space ahead of general elections in 2018. Since 2016, Government officials have made threats to restrict social media. In 2016, President Mugabe indicated his government's desire to employ 'Chinese style internet censorship' in Zimbabwe by filtering the internet and blocking social media.[180] Similar sentiments had been echoed by the ICT minister in July 2016.[181]

In September 2017, the following Whatsapp message circulated in Zimbabwe:

"In the next 3 to 5 days things may get very bad. Stock up any food or other basic commodities you may need. The Inflation rate has gone up to 50 percent it means the prices of stuff will be doubling at least once per day. The minister of finance printed excess bond notes to buy US Dollars off the streets early this week so the market may be flooded with useless money. Most shops may no longer be taking swipe transactions because of this further rise in bond note circulation brace yourself for tough times ladies and gentlemen."[182]

On 24 September 2017, the Minister of Home Affairs issued a Press Statement stating that the Whatsapp message was false, warning that spreading of alarm and despondency is a criminal offence punishable by law.[183] Similar threats were issued by Ministers Chinamasa, Bhima, and Mushowe prompting MISA Zimbabwe to issue a statement condemning the threats as unlawful due to their chilling effect on freedom of expression.[184]

Against a background of these veiled threats, on October 9, 2017, President Robert Mugabe created the Ministry of Cyber Security, Threat Detection and Mitigation which is headed by Patrick Chinamasa.[185] Various commentators have expressed worry over the development fearing that the government wants to clamp down on freedom of expression and social media as Zimbabwe gears for 2018 watershed elections.[186] As if to confirm the fears, on November 3, 2017, Zimbabwe authorities arrested Martha O'Donovan, an American Citizen working with a Zimbabwean media organisation and charged her with two counts of 'subverting constitutional government as defined in section 22(2)(a)(i) of the Criminal Law (Codification and Reform) Act' and 'undermining authority of or Insulting President as defined in section 33(2)(b) of the Criminal Law (Codification and Reform) Act'.[187]

The particulars of the first count alleged that between February 6, 2017 and November 2, 2017, Martha O'Donovan 'systematically sought to incite political unrest through the expansion, development and use of a sophisticated network of social media platforms as well as running accounts namely Magamba Network Trust @Matigary and @OpenParlyZw which she operates together with different users with a view to overthrow or

[179] *MISA Zimbabwe et al v Minister of Justice et al* CCZ/0715, http://bit.ly/2gw79XH
[180] L.S.M. Kabweza, "Chinese style internet censorship coming to Zimbabwe – President Mugabe," TechZim, April 4, 2016, http://bit.ly/2xXhpTO
[181] Nigel Gambanga, "Minister of ICT says Zimbabwean government will consult citizens if need to regulate social media arises," TechZim, July 20, 2016, http://bit.ly/2zvBSeG
[182] Rufaro Madamombe, Home Affairs Minister threatens to arrest people spreading message that basic commodities will disappear in shops, ***Techzim***, 24 September 2017, http://bit.ly/2z0RSt9
[183] Dr. I.M.C. Chombo, MP, Minister of Home Affairs, Press Statement, 24 September 2017
[184] MISA Zimbabwe, Threats Against Social Media Unlawful, 29 September 2017, http://bit.ly/2l7zetp
[185] MacDonald Dzirutwe, 'Zimbabwe's Mugabe creates cyber ministry in cabinet reshuffle *Reuters*, 9 October 2017, http://reut.rs/2yCbm77
[186] Bulawayo24News, *Zimbabwe media groups fret over Cyber ministry,* 15 October 2017, http://bit.ly/2itrUas
[187] LSM Kabweza, Activist, O'Donovan, charged for attempting to overthrow Zimbabwean government using Twitter, *Techzim*, 5 November 2017, http://bit.ly/2ArqQIb

attempt to overthrow the Government by unconstitutional means'. The particulars confirmed that the Zimbabwean authorities had been monitoring online activity in Zimbabwe, particularly content that is considered to be critical of the Government.

On 22 October 2017, the Police managed to trace the IP address that had accessed the Twitter account @Matigary to an Apple MacBook computer that belonged to O'Donovan. It was therefore alleged that O'Donovan 'engaged in working to raise foreign funding to capacitate a sophisticated online programme of action that is designed to culminate in online activism translating to an offline uprising'... to 'replicate offline uprisings like what happened in Tunisia and Egypt'. It was further alleged that O'Donovan was 'the mastermind behind an organised social media campaign aimed at overthrowing or attempting to overthrow the Government by unconstitutional means'.

The particulars of the second count alleged that O'Donovan who was one of the Administrators of a Twitter account called @Matigary posted a message on Twitter which read "we are being led by a selfish and sick man". The message had an attachment of a photo of President Robert Mugabe and a portrait illustration purporting that the President is surviving on the use of a catheter in passing out urine. The authorities considered the message 'abusive, indecent or obscene and aimed at Undermining Authority of or Insulting President'.

It is becoming apparent that the Zimbabwean Government has taken a hard stance against freedom of expression online. This sequence of events demonstrates the government's position on the citizens' use of social media to express themselves and to access information, a position which position goes against the letter and spirit of the Zimbabwe constitution that guarantees the exercise of freedom of expression by the citizenry.[188]

Digital Rights Profile:

There have been specific digital rights violations in Zimbabwe mainly relating to arrests for posting content online. On February 1, 2017, Pastor Evan Mawarire, a Zimbabwean anti-corruption activist who led #ThisFlag protests in 2016 – which encouraged Zimbabweans via social media to hold protests against President Robert Mugabe for corruption and economic crisis – was arrested by the Zimbabwe Republic Police on return from the United States where he had sought refuge months earlier. He was charged with "subverting a constitutional government". It was claimed that the pastor had been "inciting Zimbabweans from all walks of life either locally or internationally to revolt and overthrow a constitutionally elected government". Included in this were allegations that Pastor Evan Mawarire incited some Zimbabweans living in the US and "all over the world" through social media to converge in New York on September 22, 2016, to "confront" President Mugabe, who was attending the United Nations General Assembly and order him to "immediately" resign from his position for destroying the country. The case is still pending in courts.[189]

On September 23, 2017, Pastor Mawarire circulated another video on social media in which he yet again criticised Zimbabwe's economic policies and urged Zimbabweans to revolt against them. He was subsequently arrested

[188] MISA Zimbabwe, *New Cyber Security Ministry: About Trust and Respect for Rights,* 10 October 2017, http://bit.ly/2yIujo0
[189] Worldwide Movement For Human Rights, Zimbabwe: Arbitrary arrest, subsequent release and ongoing judicial harassment against Pastor Evan Mawarire, 29 September 2017, http://bit.ly/2z0moDp

and charged with 'subverting a constitutional government' under Section 22(2) of the Criminal Law (Codification and Reform) Act, Chapter 9:23, only for the charges to be later dropped by the State.[190]

There have been several arrests of journalists for doing their work using offline platforms. Although the arrests have not emanated from what journalists have said online, it is a clear indication that online journalists risk arrests if they write stories considered by government to be in bad taste. On March 3,2017, the editor of Newsday Wisdom Mdzungairi and reporter Richard Chidza were charged with insulting or undermining the president following publication of a story about President Robert Mugabe's health.[191]

On 2 October 2017, News Day published a story that Zimbabwe's First Lady, Grace Mugabe, had donated used underwear to Zanu PF supporters.[192] Following the publication of the story, Kenneth Nyangani, the author of the story was arrested and charged with criminal nuisance. Amnesty International condemned the arrest describing it as government's tactic to intimidate and harass journalists to deter them from doing their work.[193] Nyangani was released on bail pending trial set for October 18, 2017.[194]

[190] Worldwide Movement For Human Rights, Zimbabwe: Arbitrary arrest, subsequent release and ongoing judicial harassment against Pastor Evan Mawarire, 29 September 2017, http://bit.ly/2z0moDp
[191] MISA Zimbabwe, NewsDay Journalists Charged over Mugabe Health Story, 3rd March 2017, http://bit.ly/2xYvOKH
[192] NewsDay, *Grace Donates used underwear,* 3 October 2017, http://bit.ly/2l9tcly
[193] Amnesty International, Zimbabwe: Journalist arrest tactic to intimidate him and others for doing their work, 3rd October 2017, http://bit.ly/2yHqUWd
[194] Clayton Masekesa and Obey Manayiti, Newsday Underwear Reporter Granted Bail, *NewsDay,* 5 October 2017, http://bit.ly/2irlgI4

Conclusion:

Time To Find A Solution To Internet Shutdowns Is Now, And Why Internet Businesses May Hold The Key

In 2016, there were at least 13 cases of Internet shutdowns in Africa. In 2017, there have been 8 as at the time of publishing this report, and gauging from the trends of the last 2 years, there is a strong possibility that the trend of Internet shutdowns in Africa will continue in 2018. African nations have acquired a bad reputation of implementing Internet shutdowns around political events such as elections. In 2017, there were Internet disruptions in Cameroon, Togo, Morocco, Mali, Democratic Republic of Congo, Senegal, Somaliland (autonomous region of Somalia) and Ethiopia. The Internet shutdowns of 2017 all occurred around political events, with the exception of Ethiopia where Internet connections were also disrupted to prevent the leakage of high school examination results.

This is a concern because 2018 is a major election year in Africa, with at least 6 Presidential elections[195] scheduled to be held in Cameroon, Madagascar, Mali, Sierra Leone, South Sudan and Zimbabwe and Parliamentary or

[195] Electoral Institute for Sustainable Democracy in Africa. "2018 African Election Calendar". http://www.eisa.org.za/calendar2018.php

Provincial elections in 16 African countries. There were Internet disruptions in 4 of the countries/regions scheduled for Presidential elections in 2017 – Cameroon, Mali, Somaliland and South Sudan – as was the case in 2016 the Internet disruptions occurred around elections.

An immediate priority going forward in 2018 is for all stakeholders working in the digital rights community to urgently find a solution to the persistent problem of Internet shutdowns in Africa. As revealed by the stories and records of personal and national losses caused by Internet shutdowns, in light of Africa's great developmental challenges, the continent can ill afford a day of Internet shutdown in 2018. It is evident that Internet shutdowns are slowly emerging as a developmental threat to Africa, and all efforts so far to curb this threat through civil society advocacy alone is yet to produce desired results. High level declarations from the United Nations Human Rights Council on the negative effect of Internet shutdowns on nations have also had little sway on the decisions of African governments.

While the efforts of civil society and the United Nations are commendable, a viable route to at least reduce the incidents of Internet shutdowns in Africa, and stemming digital rights abuses, may be through partnership with Internet businesses. Telcos, ISPs, social networking platforms, content producers and all other Internet businesses must take on a greater and more visible role if governments in Africa are to take digital rights seriously. Their financial power is a great leverage which governments across Africa acknowledge and which they must begin to use to improve the situation around digital rights in Africa. Afterall, a country that respects digital rights is good for business because it at least ensures that losses due to shutdowns or customer dissatisfaction because of service denial or disruption are off the table.

While their on-going efforts are commendable, Internet businesses, as important stakeholders in the digital rights community, must do more and take a more public stance in the defence of digital rights. When policies and laws undermining Internet freedom are being passed, when citizens and journalists are being arrested for social media posts, when illegal mass surveillance chills freedom of expression online, when Internet connections get disrupted

for days on end, Internet businesses are often the first to feel the impact because of lost business. Using guidelines on how best to engage with government such as that developed by AccessNow[196], they can also be the prime movers in ensuring that citizens all around Africa have their digital rights respected. The year 2018 presents new opportunities in this regard.

Also, an important point to be noted by civil society is the trend of Internet shutdowns in Africa. In the past two years of our report, there have been 7 separate Internet disruptions in 5 central African nations: twice in Congo DRC and Cameroon and once each in Chad, Gabon and the Republic of Congo. In West Africa, there have been 5 Internet disruptions in 4 nations: twice in Mali, and once each in Gambia, Senegal and Togo. In North Africa, there have been 3 Internet disruptions in 2 nations: twice in Morocco and once in Algeria. In East Africa, there have been 3 Internet disruptions in 3 nations/regions: once each in Uganda, Somaliland and South Sudan while in Southern Africa there has been one Internet disruption in Zimbabwe.

[196] Dada T and Micek P, "Election watch: If Kenya orders an internet shutdown, will telcos help #KeepItOn?" Access Now, July 26 2017. http://bit.ly/2gC14cH

What this trend confirms is that Central Africa is still a hotspot for digital rights violations in Africa, and should continue to be a focus for civil society action. In this regard, in our expansion work into Africa, Paradigm Initiative is building capacity for advocacy in the region through a regional program and a mentorship scheme that will help identify (and empower) new digital rights advocates in the region.

If the events from the past 2 years are indicative of a trend, we can expect 2018 to be a busy year for digital rights advocacy in Africa. At Paradigm Initiative, we hope that our research report, country analyses and recommendations based on our work across Africa, inform the advocacy work of other civil society actors, as we all continue to be vanguards for the defence of digital rights and Internet freedom in Africa.

\\

Acknowledgements

Paradigm Initiative *Digital Rights in Africa* Report team:

Babatunde Okunoye	Research Assistant
'Gbenga Sesan	Executive Director
Innocent Kalua	Google Policy Fellow
Olumide Alabi	Graphic designer

Paradigm Initiative wishes to acknowledge the following contributors and experts who provided country insight and feedback through their responses to our survey:

Elmahjoub Dasaa	Journalist and researcher at Arrabita Mohammadia Des Ulamas
Yasmine Bilkis Ibrahim	Founding Director, Girl Up Vine Club Sierra Leone
Ababacar Diop	President, Jonction Senegal
Darcia Dieuveille Kandza	Project Assistant, Azur Developpement, Republic of Congo
Ladislas Yassin	Coordinator, Rwanda Youth Clubs for Peace Organization
Kenyi Yasin Abdallah Kenyi	Co-founder and Executive Director,The Advocates for Human Rights and Democracy, Juba, South Sudan
Mohamed Ibrahim	Head of National ICT and Digital Economy Office, Internet Society Somalia
Precious Gaye	Liberia
Elizabeth Orembo	Kenya ICT Action Network (KICTANet)
Michael Ilishebo	Cybersecurity specialist, Zambia
Chenai Chair	Researcher, Communications Manager, Evaluations Advisor, Research ICT Africa
Kathleen Ndongmo	Anqhore consulting, Cameroon
Nashilongo Gervasius	Research Director, NamShuwe Hive Namibia
Aireni Omerri	Founder, Information Security for Africa (ISfA)
Koliwe Majama	Program Officer, Media Institute of Southern Africa
Vivian Affoah	Media Foundation for West Africa (MFWA)
Richard Chisala	Founder and CTO, C3, Malawi