Constricting Freedom of Expression Online: Annual Report on the State of Internet Freedom in Africa 2017

With Funding Support from

ifex
This publication is available for public use. It can be reproduced or quoted provided the African Freedom of Expression Exchange (AFEX) is appropriately referenced.

Published by African Freedom of Expression Exchange (AFEX)
Media Foundation for West Africa (MFWA)
30 Duade Street, Kokomlemle,
P.O.Box LG 730 Legon, Accra-Ghana
Telephone: +233(0) 302 2424 70
Twitter: @AFEXafrica
Facebook: African Freedom of Expression Exchange
Email: info{@}africafrican.org
Website: www.africafrican.org

Disclaimer
This report is made possible with funding support from Toronto-based IFEX. The content of this report, however, are the sole responsibility of the author and do not necessarily reflect those of IFEX.
About the African Freedom of Expression Exchange

The African Freedom of Expression Exchange (AFEX) is a continental network made up of some of the most influential media rights and freedom of expression organisations across the West, East, Central and Southern Africa regions. Since its establishment in December 2013, AFEX, through its advocacy continues to promote free speech (offline and online) and human rights on the continent. The network is currently made up of thirteen (13) members that are all members of the Toronto-based global free expression network, IFEX. While some of the member organisations work in specific countries, others work across sub-regional blocs.

Our Member Organisations

Africa Freedom of Information Centre (AFIC)

Association for Media Development in South Sudan (AMDISS)

Centre for Media and Peace building (CEMESP)

Freedom of Expression Institute (FXI)

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

Institute for Media and Society (IMESO)
International Press Centre (IPC)

Journaliste en Danger (JED)

Media Foundation for West Africa (MFWA)

Media Institute of Southern Africa (MISA)

Media Rights Agenda (MRA)

National Union of Somali Journalists (NUSOJ)

West Africa Journalists Association (WAJA)
Content

Foreword..........................................................................................................................vii
Executive Summary........................................................................................................ix
Introduction....................................................................................................................1
2017 Internet Ecosystem in Africa..................................................................................2
Evidence gathering procedure.......................................................................................6
The Evidence...................................................................................................................9

1. Forms of online rights violations...........................................................................9
   i. Arrests and Detentions.......................................................................................10
   ii. Attacks, Threats and Cyber bullying/Cyber harassment..............................11
   iii. Internet Shutdown and censorship..............................................................13
   iv. Surveillance.....................................................................................................16
   v. Hacking/Cyber crime......................................................................................17

2. Issues implicated in online rights violations......................................................18
   i. Dissenting views and anti-government protests.............................................18
   ii. Misinformation...............................................................................................19
   iii. Nudity and revenge porn.............................................................................20
   iv. Defamation......................................................................................................21
   v. Vulgarity and deviations from socially accepted norms..............................21

3. Actors in online rights ecosystem.......................................................................22
   i. Perpetrators......................................................................................................24
   ii. Victims............................................................................................................26
   iii. Advocates and Facilitators..........................................................................27

Conclusion....................................................................................................................29
Recommendations..........................................................................................................30
Appendix.......................................................................................................................34
The Internet has brought cyberspace to the doorsteps of people, whether they are high and mighty or low and disadvantaged, enabling them to engage actively in public discourse on political, social and economic issues, among others at local, national, regional and international levels.”

Edetaen Ojo,
Chair, AFEX Steering Committee
Given the important role that the Internet plays in empowering citizens to actively engage in governance and issues of interest and concern, there has been a call for governments and stakeholders to prioritise Internet access and use in their respective countries. Over the past decade, internet enabling devices have become increasingly accessible to citizens, empowering them to participate in national discourse, demand better public service delivery, and for many other purposes. Despite these benefits and opportunities that the Internet presents, many governments in Africa tend to control the cyberspace by adopting laws, policies and practices that seek to limit the freedoms that people enjoy online.

As part of its efforts to help counter this threat to Internet freedom, the African Freedom of Expression Exchange (AFEX) has put together this report which tracks incidents and developments recorded in 12 African countries in 2017. The findings of this maiden “Annual Report on the State of Internet Freedom in Africa” show that there are increased threats to the enjoyment of Internet freedom and rights on the continent.

While significant efforts have been made by some African governments to guarantee these rights, other governments have increasingly adopted laws, policies and practices aimed at constricting the cyberspace for the enjoyment of Internet rights and freedoms. Journalists and other media practitioners, bloggers, human rights defenders and ordinary citizens have been targets of abuses such as arbitrary arrests and detentions, physical and verbal assaults, prison terms and fines for exercising their rights online.

There were a total of 36 incidents recorded in which online expression was criminalised through arrest and detentions, prison terms or fines. Nigeria recorded the highest number with 13 such incidents in which online expression was criminalised.

Internet shutdowns were also used especially during important events like elections or protests or during terror attacks or national emergencies to silence dissent and curtail freedom of assembly rights. Nine incidents of Internet blackout were recorded in five countries with some experiencing multiple shutdowns.
Security agents, ruling and opposition parties and politicians, media regulatory bodies, and individuals were identified as the perpetrators of the majority of violations recorded. It was also observed that most of the violations recorded did not receive any form of redress actions.

It was also observed that there was increased civil society advocacy on Internet freedom in Africa.

The report concludes with recommendations to key stakeholders in the Internet ecosystem on the African continent such as governments, media, civil society, technical community and the general public. The recommendations urge state and non-state actors to prioritise the Internet and the opportunities it presents by ensuring a free and protected space for all to exercise their rights.

Edetaen Ojo,

Executive Director, Media Rights Agenda, Nigeria
Chair, Steering Committee of the African Freedom of Expression Exchange (AFEX)
Executive Summary

Although the Internet is increasingly becoming a powerful space and medium for information sharing and self-expression on the African continent, there appear to be increased threats to the enjoyment of Internet rights and freedoms on the continent.

The liberalising and empowering function of the Internet has opened up duty bearers to higher levels of scrutiny, thereby forcing demands for transparency on them. Citizens, particularly journalists, bloggers, social and political activists, have all taken to online-based platforms to have their voices heard, as they demand their due from duty bearers, a condition that unfortunately, exposes them to attacks. Unaccustomed to these new vulnerabilities, political and economic elites react with repressive laws, threats, attacks, and the curtailment of access to and use of internet resources.

This is not to say that all is well with non-elite elements within Africa’s digital ecosystem. Indeed, some persons and entities abuse the power of the internet and infringe on the online rights and freedoms of others. However, attempts to control such excesses should not, in themselves, initiate and perpetuate a vicious cycle of violation, repression and polarisation.

Key recommendations from the research and the findings include the following:

African Governments (and governance machinery including ministries, regulatory agencies etc.), should:

- Repeal laws that repress free expression and adopt international legal provisions that protect citizens’ digital rights and freedoms.
- Undertake broad-based consultations with media, civil society and other relevant stakeholders in the formulation of laws and policies
related to digital rights and freedom of expression.

- Improve transparency and responsiveness in the provision of information about violations under investigation.
- Facilitate the activities of CSOs and media organisations that monitor violations of the right to freedom of expression online.

**Regional and international blocs including AU, UN, ECOWAS, etc., should:**

- Develop and strengthen diverse mechanisms for sanctioning states which resort to violations.
- Co-ordinate and deploy strong, international, and public condemnation of States involved in the violation of the right to freedom of expression and digital rights.
- Facilitate the visits of UN and AU Special Rapporteurs on Freedom of Expression to monitor and review digital rights ecosystems on the African continent.

**Industry players (e.g. telecommunication operators and Internet Service Providers) should:**

- Should uphold the rule of law by challenging unlawful requests from governments.
- Should develop and adopt clear due diligence mechanisms, especially ISPs, to manage internet shutdown orders and other unusual requests made by African Governments.

**Technical community should:**

- Build and make available resilient digital solutions that will make it more difficult and cumbersome for governments to resort to violations such as unwarranted internet shutdowns and surveillance.
Introduction

The Internet has become an indispensable tool in enabling citizens to enjoy their rights to free expression, which is now accepted as an enabler of other rights. It has also contributed to increased citizen participation in public discourse on issues of interest in different countries around the African continent and beyond.

For instance, through the Internet, citizens can easily mobilise for protests, debates, meetings and a range of other activities in response to issues that affect them. The Internet has also expanded economic activities by providing a platform for buyers and sellers who are spatially removed from each other to be able to transact businesses. Its ability to close up geographical gaps also means that it is a useful tool for connecting people for reasons other than civic actions and business.

In Africa, as in the rest of the world, the proliferation of Internet-enabling devices such as mobile phones, computers and laptops, and the emergence of social media platforms has made it easier for everyone, including the rich and poor, the educated and uneducated, the employed and unemployed, to benefit from the power of the Internet. Across African countries, although Internet penetration has been very low for many years, it is fast rising. The frontrunner in this is Nigeria which has achieved parity between those with access and those without. Indeed, data available from the industry regulator in Nigeria, the Nigerian Communications Commission (NCC), indicates that as at February 2018, there were 100,904,668 mobile telephone lines in Nigeria with active Internet subscriptions\(^1\) in a country which currently has a population of an estimated 190 million. Undoubtedly, significant

\(^1\) [https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5](https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5)
progress has been made towards bringing the Internet to the doorsteps of ordinary citizens.

Despite these gains in access and the numerous opportunities that the Internet presents for citizens, there remain critical challenges that interfere with citizens’ ability to use the Internet to exercise their civil rights.

This report presents a synthesis of incidents and developments on the continent in 2017 that have implications for citizens’ ability to leverage the opportunities presented by the Internet. The report is organised in four main sections. It begins with an overview of the Internet ecosystem on the continent as gathered from 12 African countries. This is followed by an explanation of the procedure used in assembling the evidence presented in the report. The third section presents the evidence gathered through a thematic discussion of certain key issues. It then concludes with a number of recommendations for future actions by relevant stakeholders.

### 2017 Internet Ecosystem in Africa

Generally, Internet penetration levels across the countries observed remain low compared to the picture presented by countries in the global North. Among the countries sampled, Nigeria has the highest Internet penetration with about 47% of the population being able to access it. While this is an impressive showing on the continent, the figure is far lower than that of countries such as the UK which has almost 100% coverage among some demographics (Office for National Statistics, 2017).\(^2\) Nigeria is closely followed by Uganda while countries such as Ghana, Cote D’Ivoire and Cameroon hover in the middle. Somalia was trailing behind in the Internet penetration journey with only two per

---

cent of its population having Internet access. Following years of civil war, Somalia’s entire telecommunications sector collapsed and therefore presents no surprises in the low Internet penetration levels. Interestingly, they presently offer some of the most technologically advanced and competitively priced telecommunications and Internet services in the world.³

Across the countries observed, Internet services are being provided by combinations of public and private industry players. For instance, in Togo, there are two mobile operators (state-owned TogoCel and privately owned MOOV) and two Internet Service Providers (Togo Telecom and Café Informatique). In The Gambia, the telecoms sector has Gamcel (state owned) and Africell (foreign-owned), Comium (foreign-owned) and Qcell (private, domestic). Similarly, in Liberia, the players are MTN-Lone Star (Private), Cellcom (Now Orange; private) and Libtelco (state-owned). In a few instances such as Ghana, which also registers some of the most liberal legal postures towards free expression, the sector is fully liberalised and in private hands with state regulators’ oversight. Internet speed remains relatively slow and costs are high even to the point of driving citizens to protest for better services and demand a reduction in cost of Internet services as was witnessed in Zimbabwe’s #datamustfall protest against Internet service price hikes.

For the most part, Internet service access and use appears to be closely tied to the rising uptake of mobile telephony as demonstrated by countries such as The Gambia and Ghana where mobile phone uptake is well over 100 per cent (ICT Development Index, 2016).⁴ However, the Internet culture, whether via mobile phones or other receiver tools, is largely also

youth-oriented meaning that substantial numbers of the older population
are left out. Younger people are increasingly using Internet services
available in their countries to access social media in pursuit of varied
intentions. Social media platforms such as Facebook and WhatsApp are
extremely popular across the countries sampled and serve as the main
platforms for people giving expression to their citizenship. African
citizens take to social media to expose corruption, complain about things
they are dissatisfied with or even to malign others, as seen in the country by
country evidence presented in Appendix 1. As exemplified by the many
attacks on bloggers in the evidence presented, African citizens are also
taking to blogging.

Our observations also point to two main models for regulating the
online space and managing the enjoyments of rights thereon. First
is legislation by which governments and parliaments on the continent
have sought to exercise control over online expression. There are still
a number of repressive laws that criminalize online expression as is
the case in Nigeria’s Cybercrime Act (Sections 24 and 38) portions
of which have been widely criticized as repressive. Such laws are
often deployed as the basis for arrests for comments made online. Given
their usefulness to the political elite, these laws often withstand pressures
from civil rights groups advocating for their repeal or amendment.

In Zimbabwe, although President Mugabe had said that the Cybercrimes
law would be enacted by 2017 it remained at the Attorney General’s
office (Bill Watch, 2017). The government continued to rely on
unconstitutional laws to suppress online freedoms. In some instances,
such attempts at securing amendments have yielded results. For instance,
in Cote d’Ivoire, a 2016 Press Bill which sought to criminalise online and
offline speech was revised to exclude the repressive sections following pressures from CSOs before it was passed in December 2017.

On the one hand, some regulatory frameworks protect individual rights to free expression online. Countries such as Togo have, for instance, pushed for laws that facilitate the freedom of the Togolese people to access public information both online and offline. Ghana already has liberal laws that allow for the protection of fundamental rights to freedom of expression online. Ghana’s Data Protection Law (2012) has been described as one of the best that guarantee citizens’ rights in the country. In other countries like Nigeria, civil society groups have also been instrumental in putting pressure on the government to adopt the Digital Rights and Freedom Bill to guarantee human rights online. The Bill has been passed by Nigeria’s bi-cameral legislature, having been passed on December 19, 2017 by the lower chamber of the House of Representatives, and by the upper chamber, the Senate, on March 13, 2018. The Federal Parliament of Somalia also passed a National Communications Act on August 9, 2017 to, among other things, provide for the creation of a telecommunications authority, which would regulate the sector and provide protection for corporate and consumer rights (Horn Observer, 2017).

Evidence gathering procedure


The evidence presented in the report is based on incidents of online violations/threats and notable trends and developments from 12 African countries. The countries cited in this report are Cote d’Ivoire, Ghana, Togo, Liberia, Ethiopia and Nigeria. The other countries include Cameroon, Somalia, the Democratic Republic of Congo, The Gambia, Uganda, and Zimbabwe. The 12 target countries were selected based on AFEX’s presence there as well as the occurrence of incidents of violations/threats or online media developments during the monitoring period.

The data was collated by AFEX member organisations using a combination of evidence gathering methods. These include incident reports, online monitoring and news analysis by the network partners. In addition, where the AFEX network has no representation in a particular African country, reports published on the IFEX, formerly International Freedom of Expression Exchange website by other human rights organisations are also included.

The report covers incidents of online rights violations; responses and interventions by both state and non-state actors as well as an analysis of the patterns forming around these core issues (see Figure 1).
It is presented, subsequently, in three sections. The first section presents a brief overview of the digital landscape of the 12 countries represented in the report (see Table 1). This is followed by the empirical evidence that serves the basis of the report. The third section presents a synthesis of the patterns forming around the individual events. Finally, the report concludes with recommendations to various stakeholders within the digital ecosystem.
<table>
<thead>
<tr>
<th>Incidents</th>
<th>Nigeria</th>
<th>Togo</th>
<th>Cote D'Ivoire</th>
<th>Ghana</th>
<th>Gambia</th>
<th>Liberia</th>
<th>Zimbabwe</th>
<th>Cameroon</th>
<th>DRC</th>
<th>Uganda</th>
<th>Ethiopia</th>
<th>Somalia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminalizing Speech: Arrests/Detention/Sentencing</td>
<td>13</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Online harassment/Trolling Threats</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Censorship/Shutdowns</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Surveillance</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Engendering online rights/Civil Society Efforts</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Coercive posture to online free expression</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hacking</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The Evidence

1. Forms of online rights violations

A cursory look at the evidence gathered shows that violations of individuals’ rights to free expression online take varied forms as demonstrated by the word cloud of key action words in the data gathered (see Fig 2). As explained below, these violations include arrests and detention, online harassment, hacking and Internet shutdowns. There have been reports in recent years, including in 2017, of the monitoring of online communications of citizens, and widespread use of mass surveillance. However, because many citizens are often unable to tell when their online communications are being monitored and their privacy rights violated, such activities frequently go unreported.

Figure 2: Word cloud of online rights violation forms
i. Arrests and Detentions

In many of the countries monitored, citizens continued to face the risk of being arrested, detained and/or prosecuted for exercising their right to free expression online. Unfortunately, duty bearers and the political elite often interpret criticisms and other forms of legitimate expression as demonstrating intention to disrupt peace and upset their preferred status quo. State security agencies, often acting at the instance of the political elite, tend react to such behaviours with detention, arrests and prosecution under broad and vaguely-defined laws. For instance, in May, a prominent Ethiopian opposition activist, Yonatan Tesfaye, was arrested and sentenced to six and a half years in prison, on terrorism charges. His charges related to Facebook posts in which he criticised the government’s handling of the Oromia protests. Indeed, in some cases, victims even suffer torture during the period of detention as was the case of Lance Corporal Samboujang Bojang, one of four soldiers arrested in The Gambia by Military Police for joining a WhatsApp group accused of mutinous intentions. He was detained without the benefit of a court appearance only to be hospitalized upon his release for alleged torture at the hands of the security operatives.

As the most likely victims of attacks on free speech, journalists are not left out of this mode of online rights violations. For instance, in Nigeria alone there were six instances of arrests of journalists and broadcasters in 2017. This excludes bloggers and social media activists with active following. Uganda and Zimbabwe recorded three and two such arrests respectively. Similar cases were observed in Somalia, Ethiopia and Cameroon.
Two Ugandan journalists, Stanley Ndawula and Robert Ndawula in the dock on October 30, 2017; they were accused of malicious publications under the Computer Misuse Act 2011.

ii. **Attacks, Threats and Cyber bullying/Cyber harassment**

Online rights violations also took the form of attacks and threats, in response to a person’s online posts or comments that resulted in physical or emotional harm, death or placed victims in unreasonable fear. Such attacks were meted out either online or offline. Major forms of the online-based attacks included trolling (inflammatory, insulting, or extraneous comments intended to upset or provoke someone) and revenge pornography (illegal dissemination of nude pictures and videos of persons without their consent with a view to embarrassing them).
Examples on such online attacks were recorded in Côte d’Ivoire where youth leader and self-declared ‘Celibbattante’ (single but able woman) Nancy Ndri, was the target of abuse and harassment from several Internet users. A popular Ivorian singer, Josey, also suffered a similar fate for her affair and pregnancy with an Ivorian footballer. In Ghana, a displeased husband, Lawrence Abrokwa, took to social media to circulate a nude video of his wife, Afia Schwarzenegger, a television presenter and actress in an apparent attempt to humiliate her. A similar case of revenge pornography was recorded in The Gambia where Fatou Manneh was fined 10,000 Dalasi ($200) or in default, to serve a prison term of one year for disseminating nude pictures of a complainant on WhatsApp.

Offline attacks on individuals for exercising their free expression rights online include incidents of physical or verbal assault, threats and intimidation. Many media practitioners, activists and ordinary citizens who expressed dissent online became targets of unlawful violence. In Nigeria, Police on January 19, 2017, raided offices of Premium Times, an influential news website, after the Chief of Army Staff accused the website of defamation. Also, in Côte d’Ivoire, a former minister under the government of Ouattara, Alain Lobognon, was threatened and the police sent to his house to intimidate him following his tweets which were deemed critical of the government. Similarly in Uganda, Stella Nyanzi, a human rights activist was arrested and accused of cyber harassment against President Museveni under the Computer Misuse Act 2011. Nyanzi had criticised the President and his wife over a campaign in which she called for government to fulfil its promise of providing free sanitary pads to school girls in the country.
It is worth noting that, some of the violations cited in this report were also perpetrated by non-state actors. In a related development in the incident cited above, unknown assailants kidnapped and physically assaulted Gertrude Uwitare, a reporter with NTV in Uganda, for her blog post in which she defended Nyanzi’s comments. The unknown assailants shaved Uwitare’s head, beat her and even threatened to torture her. She was released after 12 hours.  

In another incident recorded in Nigeria, a group of individuals in Abakaliki, a town in Ebonyi State physically attacked Charles Otu, a journalist working with *The Guardian* newspaper for critical Facebook comments he made about the Ebonyi State government.

### iii. Internet Shutdown and censorship

In terms of restrictions to digital and online freedom of expression rights, another emerging phenomenon is the tendency for governments to authorise complete or partial Internet shutdowns or content censorship. Access Now, a leading CSO that promotes digital rights, defines Internet shutdowns as the “intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location often to exert control over the flow of information” (Access Now, 2017). This practice is especially worrying considering the immense power the Internet has in contributing to the attainment of the sustainable development goals (SDGs) in spheres ranging from health, education and economic growth to climate action, peace and good governance. Several governments (Somalia, Ethiopia, Uganda, DR Congo, Cameroon, Zimbabwe, Liberia, Togo and Nigeria)

---

8. [https://www.accessnow.org/keepiton](https://www.accessnow.org/keepiton)
resorted to Internet shutdowns or content censorship as a means to disrupt anti-government protests and check the spread anti-government content.

For instance, on two occasions, the Cameroonian government shut down Internet access to the country’s North-west and South-west regions in an attempt to stifle protests against political and economic discrimination. The first Internet blackout which lasted 94 days deprived about 7 million citizens access to information and resulted in economic loss of about U.S. $ 4.5. The second shutdown lasted about 150 days.⁹

---

 Sadly, in August 2017, authorities in DRC ordered Internet service providers to intentionally slow down Internet connection to make it difficult for the transmission of images on social media platforms. Again in December 2017, the Congolese government authorised a complete nationwide Internet shutdown and disruption of SMS services in a crackdown a day before the scheduled protests by activists of the...
country’s Catholic Church. Similarly, the Togolese government on two occasions in September 2017 ordered a country-wide Internet shutdown during anti-government protests. In Ethiopia, the government cited the need to prevent exam leakage as justification for Internet shutdowns.

In October 2017, without any sort of due process, the Nigerian Communications Commission (NCC), acting on the instructions of the National Security Adviser to the President ordered several privately-owned Internet service providers (ISPs) to “restrict access” to 21 websites alleged to be “websites threatening national security as identified by the Office of the National Security Adviser”\textsuperscript{10}. By a letter dated October 20, the NCC directed the ISPs to restrict access to the websites by blocking their domain names and gave the ISPs seven days to report back to it. Apparently, a similar letter had been written to several ISPs on September 27 directing them to block access to the websites of an unknown number of online publications and activist organizations.

\textbf{iv. Surveillance}

In close relation to the use of Internet shutdowns is the rising trend towards surveillance of individuals’ online comments and posts. There are growing concerns on the continent about government surveillance that threatens citizens’ right to privacy and freedom of expression. In particular, such concerns have been articulated about equipment at the new National Data Centres in Zimbabwe which were sourced from China, a country that was recently found to have bugged the African Union headquarters. Similar concerns followed fears that Nigerian security agencies were putting millions of mobile phones users under

\textsuperscript{10}. file:///C:/Users/ayeboah-banin/Downloads/List\%20of\%20Websites\%20to\%20be\%20blocked\%20(1).pdf
surveillance. In June 2017, the Uganda Media Centre, the media regulatory body publicly announced a new social media monitoring unit to scan critical posts. This was soon to be followed by a report in the Daily Monitor newspaper that the government was in contact with the Chinese government to develop a cyber-security strategy with which to build the “technical capacity to monitor and prevent social media abuse”.

v. Hacking/Cyber crime

Hacking refers to the act of gaining unauthorized access to the data in a computer or network. We observed some hacking incidents targeted at institutions in some of the countries monitored. Some of the hacking incidents recorded were done to force victims to make ransom payments in order to regain access and control over data.

For instance, in August 2017, Zimbabwean Minister of Information, Communication Technology, Postal and Courier Services, Supa Mandiwanzira confirmed that two banks had been affected by ransomware cryptoworm virus, WannaCry.

In June 2017, students took to social media to report the hacking of the National University of Science and Technology (NUST) and the Harare Institute of Technology (HIT) websites by persons demanding more than $6 billion as ransom. Besides hackings by individuals for financial gain, it appears it may also be motivated by corporate sabotage. This was the case of several Internet Service Providers (ISPs) in Liberia whose 2016 malware attacks were reported (by an arrested suspect) to have been contracted by a competitor.
2. Issues implicated in online rights violations

This section addresses the nature of issues likely to be at the centre of incidents of online rights violations. From the evidence gathered, we isolate five examples of such issues—dissenting views and anti-government protests, misinformation, nudity and revengeporn, defamation, and vulgarity/ deviations from social norms. Among these, though, it appears the most prominent issue was the expression of anti-government sentiments and/or protests.

i. Dissenting views and anti-government protests

Remarks against government officials or members of the ruling class were frequently at the centre of online violations of the rights of the ‘so-called’
perpetrators. Often interpreted as attempts to incite the public against the ruling class, such expression of dissenting views was often greeted with high handedness from the political class. Across the countries monitored, there appears to be a growing impatience towards dissenting views expressed online. The arrests of several opposition elements and attempts to quell anti-government protests through Internet shut downs exemplify this issue. In almost all the countries observed a publication, tweet, blog or status update that was deemed anti-government elicited punishment either from those in authority or pro-government elements.

In Nigeria, for instance, in June, Charles Otu, a correspondent with The Guardian newspaper, was assaulted by a group of individuals in Abakaliki for Facebook comments in which he was critical of the Ebonyi state government. Also in Nigeria, 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.

In Côte d’Ivoire, a political journalist and blogger was threatened for writing a blog in which he criticized the Ivorian Speaker of Parliament, Soro Guillaume, while Fatou Badjie was arrested in The Gambia for allegedly insulting the new president and asking Gambians to stay vigilant and proactive in the fight for democratic reforms. Across Togo, DRC, Cameroon, Ethiopia and Somalia, governments also resorted to Internet shutdowns to suppress dissent with the most defaulting country in this being perhaps, Cameroon for its handling of protests in its two English speaking regions.

ii. **Misinformation**

Another issue likely to elicit violations of online rights was misinformation or feeding the public with false news on the Internet.
This issue was relatively less visible across the sample, tending only to be present in the evidence from three countries—Nigeria, Cameroon and Somalia. However, this is not to suggest that misinformation is the preserve of these countries. Indeed, in this era of fake news, misinformation is a likely phenomenon in every country. However, the evidence presented here has incidents of (suspected) misinformation which subsequently elicited rights violations against culprits and other citizens.

In Nigeria for example, on January 2, 2017, Police arrested Jerry Edoho, a journalist working with *Ibom Nation* newspaper in Uyo, for a false claim in a Facebook post that an aircraft belonging to one of Nigeria’s airlines had crashed. In Cameroon, on the eve of scheduled protests, the government shut down Internet access reportedly to curtail the spread of false information on social media capable of inciting hatred and violence in the crisis-hit regions.11

### iii. Nudity and revenge porn

During the period under review, nudity and revenge porn were quite prevalent. Whereas nudity may be shared on line by the individuals involved, revenge porn as suggested in the name is a tool used often by individuals against those with whom they have disagreements. It is interesting to note that apart from the Gambia that recorded one incident of revenge porn, Ghana was the only country with such issues. Given its legal and online decency implications, it is not surprising therefore that nudity and pornography online are often greeted with legal punitive measures. For instance, the Somanya District Police

---

Command in the Eastern Region of Ghana arrested two persons who circulated nude pictures of a 20-year old Senior High School graduate. Two university students were also arrested by officials of the Police Cyber Crime Unit for allegedly posting nude pictures of underage junior high school students on the Internet. In The Gambia, a court fined one Fatou Manneh D10,000 ($200) for disseminating naked pictures of a complainant. In default, she was to serve a prison term of one year.12

iv. Defamation

Defamation, although quite uncommon during the period under review, was relatively visible in Nigeria. Two instances of defamation were recorded in the country directed at political figures. On June 15, a journalist, Danjuma Katsina was arrested in Katsina over comments he made on Facebook questioning the legitimacy of a newly elected member of Nigeria’s House of Representatives from the state. Also, in March 2017, the Chief Magistrate court sentenced one Gambo Saeed to nine months imprisonment for defaming the governor of Katsina state. Clearly, defamation is not taken kindly and while not very common, is nonetheless, very likely to be greeted with arrests and other restrictions to free expression.

v. Vulgarity and deviations from socially accepted norms

The use of vulgar language was also an issue that sparked online violations. In Liberia, the administrators of several sites and social media groups blocked users whom they deemed to be using vulgar language. A

similar pattern was observed among radio show hosts whose programmes had banned online-based listener input which they deemed offensive. For instance, in Liberia, the Costa Show on Shaita FM, which is also streamed live, had the host frequently blocking callers who expressed contrary views. Offensive language was also at the centre of attacks by a Ghanaian police officer who made disparaging comments about the people of the Upper West Region in Ghana.

Besides offensive and vulgar language, individuals deemed to be deviating from accepted norms were likely to have their behaviours greeted with online attacks in the form of harassment, insults and intimidation.

People’s rights were often abused online when aspects of their private lives were revealed on social media and found to be ‘unacceptable’. Women stepping outside gender role boundaries such as Nancy Ndri of Côte d’Ivoire, feminists, members of the Lesbian Gay Bi-Sexual Transgender and Intersex (LGBTI) community, were all subjected to various forms of online abuse and harassment. Indeed, as reported at an August 2017 meeting by the Association for Progressive Communications (APC) in Harare, such groups view the Internet as an unsafe technology for them.

3. Actors in online rights ecosystem

Our examination of violations of free expression online invariably beckons an analysis of the major actors are in such occurrences. A violation presupposes the existence of a perpetrator and victim. In addition, emerging trends on the continent show an increasingly strong presence and involvement of civil society and rights organizations in
supporting efforts at engendering free expression online. This section of the Report unpacks the characteristics of persons/entities that fall into these three categories.

The ‘notification’ from the Ministry of Cybersecurity, Threat Detection and Mitigation. These notifications were largely false and reflect the misinformation which surrounded the activities of the ministry.
i. **Perpetrators**

The first and perhaps, the major group of perpetrators of violations against individuals’ online rights as cited in this report is mostly state actors such as security agents, regulatory bodies or authorities and political party affiliates or leaders. Across the countries sampled, individuals and institutions acting in their capacities as state agents employed or abused existing laws to limit citizens’ rights to self-expression online. From surveillance, through arrests and detentions to Internet shut downs, the evidence gathered is replete with such examples of state-inspired online rights abuse.

Interestingly, individual members of the public were also found culpable in a lot of the instances of online rights abuse. Individuals initiated trolling, revenge pornography, hacking, threats and intimidations against others for expressing themselves. As demonstrated in the section headed “Attacks, Threats and Cyber bullying/Cyber harassment”, all incidents of such rights violations recorded in Ghana were perpetrated by individuals. Côte d’Ivoire and Uganda also had examples of online rights violations that had individual members of the public as culprits.

Beyond violations by individuals, we also see signs of rights violations at the hands of loosely-connected groups and criminal syndicates. Groups of individuals, media houses, political parties, criminal syndicates, and terrorist groups were sometimes behind repression of digital rights during the monitoring period. An example of the loosely-connected individuals perpetrating online rights violation is the Nigerian case in which Charles Otu, a correspondent with *The Guardian* newspaper, was assaulted by a group of individuals in Abakaliki for his critical Facebook comments of the Ebonyi state government.
In Zimbabwe, we see such group action coming from both the ruling and main opposition political parties who limited their members’ engagements on social media. Indeed, in May 2017, the Movement for Democratic Change (MDC-T) reportedly informed its members that it would not handle grievances (of members) that were shared on social media. A month later, Zanu PF banned its members from bringing cell phones to its politburo meetings in order to curb leaks to the media.

Finally, we also see the hands of criminal syndicates and terrorist groups in operation as violators of online rights. For instance, in Somalia, extremist group, Al-Shabaab, forced Hormuud Telecom to stop its news alert via short code and SMS services used by radio stations to disseminate news articles after the latter had refused to make their services available to Al-Shabaab’s radio station.
ii. Victims

On the receiving side of online rights violations lie some very common victim types. The evidence shows that some of the most commonly and adversely affected victims of violations of online freedoms included journalists and other media practitioners, opposition activists and women.

Women were typically targeted online when they departed from socially accepted roles and norms and tended to be targeted with revenge pornography, harassment and insults. Indeed, with a few exceptions, the evidence on “attacks/threats” as a form of violation had women as victims. Examples include the cases of Nancy Ndri and Josey of Côte d’Ivoire and Afia Schwarzenegger of Ghana.

Another group most likely to be targeted for online rights violations are journalists/media practitioners. Though the ubiquity and utility of the Internet has democratised the global communication space, journalists and other media professionals still serve as one of the primary sources of information and communication. They are the vital connection between persons and information, serving the former with the means to form opinions and make decisions. In so being, they are often targeted for sharing information that is deemed defamatory to the actors therein.

Journalists and other media practitioners become targets of violations when they criticise or express their opinion, investigate and make accusations about issues and persons of public interest. Examples include threats against the Ivorian political journalist and blogger for his blog criticising the Speaker of Parliament, Soro Guillaume. In Nigeria, journalist Midat Joseph of the Leadership newspaper and Chair of the local branch of the Nigeria Union of Journalists (NUJ) was arrested for comments made in a WhatsApp group.
Five other such incidents involving journalists and media practitioners were recorded in Nigeria alone. Côte d’Ivoire, Zimbabwe, Cameroon, DR Congo, Uganda, Ethiopia and Somalia all had examples of attacks against journalists’ online rights.

A third group of potential victims of online rights abuse is opposition activists who are targeted for expressing dissenting views on the decisions and actions of the ruling class. While dissenting viewpoints are the cornerstone of any democratic system, we observed that dissidents are often met with punishments such as arbitrary arrests and detentions, threats, physical assaults, Internet shutdowns, among others. Examples of this include the arrest, in The Gambia, of four soldiers for participating in a WhatsApp chat accused of sharing mutinous content. In the Côte d’Ivoire, similar attacks targeted a Former Minister in the erstwhile Ouattara government following tweets criticising the government while in Ethiopia, Getachew Shiferaw, the editor-in-chief of a local Amharic newspaper *Negere-Ethiopia*, was sentenced to one year and six months in prison for his Facebook comments.

iii. Advocates and Facilitators

The foregoing discussion of victims and perpetrators paints a picture of gloom. However, there is a lot of hope and optimism in the fight to safeguard digital rights across the continent of Africa. This is primarily due to the work of several civil society groups, individuals and even state actors that act as advocates, facilitators and protectors of digital rights. Civil Society Organisations (CSOs) were actively engaged in influencing government actions and legislation that border on access to information and free expression, both online and offline. For instance, in Nigeria, a coalition of CSOs including Media Rights Agenda, Paradigm Initiative
and Enough Is Enough Nigeria filed a suit to challenge the constitutionality of Sections 24 and 38 of the Cybercrime Act which had been widely criticised as repressive. The CSOs, led by Paradigm Initiative, have also been instrumental in drafting and calling on the Nigerian government to adopt the Digital Rights and Freedom Bill to better guarantee human rights online.

Civil society groups also play a central role in monitoring, documenting and denouncing violations, and agitating for remedial actions against perpetrators. We see how effective such efforts can be in the case of the interventions by local rights groups in Nigeria in securing the release of Danjuma Katsina, a journalist who was arrested over comments he made on Facebook in which he questioned the legitimacy of a newly elected member of Nigeria’s House of Representatives. Again, AFEX and its members and other local and international rights groups condemned and advocated against the emerging trends of Internet shutdowns during important national events like elections and demonstrations in countries like Uganda, DRC and Cameroon. For instance, the government of Cameroon was forced to restore Internet connection in the two Anglophone regions of the country after 94 days of complete shutdown following the #BringBackOurInternet campaign on social which was widely used by local, regional and international rights groups.

It is also heart-warming to note that while government functionaries are often guilty of violations, some also championed digital rights and freedoms by facilitating an enabling environment for same. For instance, in June 2017, the government of Ghana teamed up with other stakeholders to stop the illegal circulation of viral images and videos of a young military officer who was lynched by a mob.

The governments of three African countries, Ghana, Kenya, and Tunisia,
are members of the Freedom Online Coalition (FOC), established in 2011 at the inaugural Freedom Online Conference in The Hague, the Netherlands, at the initiative of the Dutch Foreign Ministry, which consists of 30 governments that have committed to work together to support Internet freedom and protect fundamental human rights, particularly the rights to freedom of expression, association, assembly, and privacy online worldwide.

**Conclusion**

The monitoring project shows that the Internet is increasingly becoming a powerful space and medium for information sharing and self-expression on the continent. The liberalising and empowering function of the Internet has also opened up duty bearers to higher levels of scrutiny, thereby forcing demands for transparency on them. Citizens, journalists, bloggers, social and political activists etc. have all taken to online-based platforms to exercise their voice and demand their due from duty bearers, a condition that unfortunately, exposes them to attacks. Unaccustomed to these new vulnerabilities, political and economic elites react with repressive laws, threats, attacks, and the curtailment of access to and use of Internet resources.

This is not to say that all is well with non-elite elements within Africa’s digital ecosystem. Indeed, as shown by the monitoring, some persons and entities abuse the power of the Internet and infringe on the online rights and freedoms of others. However, attempts to control such excesses should not, in themselves, initiate and perpetuate a vicious cycle of violation, repression and polarisation.
Recommendations

Below, are a number of recommendations that various stakeholders may consider in addressing the odds of future online rights violations as well as promote the overall digital landscape in Africa:

African Governments (and governance machinery including ministries, regulatory agencies etc.) should:

- Repeal laws that repress free expression and adopt international legal provisions that protect citizens’ Internet/digital rights and freedoms.
- Undertake broad-based consultation with media, civil society and other relevant stakeholders in the formulation of laws and policies related to digital rights and freedom of expression.
- Commit to resource relevant security agencies to successfully investigate and punish abuse of Internet/digital rights and freedoms, irrespective of the perpetrators’ clout.
- Improve transparency and responsiveness in the provision of information about violations under investigation.
- Facilitate the activities of CSOs and media organisations that monitor violations of online free expression.

Regional and international inter-governmental organizations, including AU, UN, ECOWAS, etc., should:

- Develop and strengthen diverse mechanisms for sanctioning states which resort to violations.
- Co-ordinate and deploy strong, international, and public
condemnation of States involved in the violation of free expression and digital rights.

- Facilitate the visits of UN and AU Special Rapporteurs on Freedom of Expression to monitor and review digital rights ecosystems on the African continent.

- Support the capacity development of civil society, media organisations, regulators and other relevant governmental agencies on ways to safeguard digital rights and freedoms.

The technical community (e.g. telecommunication operators and Internet Service Providers) and other industry players should:

- Uphold the rule of law by challenging unlawful requests from governments.

- Develop and adopt clear due diligence mechanisms among telecommunication operators, especially ISPs to manage illegal Internet shutdown orders and other unusual requests made by Governments.

- Prioritise telecommunications infrastructure provision in underserved populations and geographic locations to help bridge national and local inequities in access to digital resources and opportunities

- Build and make available resilient digital solutions that will make it more difficult and cumbersome for government to resort to violations such as Internet shutdowns and unwarranted surveillance.

Civil society organisations should:

- Play a watchdog role over state activities with regards to online rights and freedoms. CSOs should monitor and remind States of their
obligations under international treaties and agreements, through advocacy and legal challenges.

• Lobby media organisations to provide digital security and self-protection training to employees or freelancers.

• Monitor and publicly condemn violence perpetrated against journalists, individuals and organizations for exercising their fundamental right to freedom of expression online.

• Encourage the Special Rapporteurs on Freedom of Expression (both at AU and UN level) to undertake official missions to African countries to assess and report on Internet ecosystems.

• Explore creative avenues to highlight beyond human rights, the other debilitating effects of repression of digital rights and freedoms. Here, economic arguments could be used in advocacy efforts.

• Enhance their own capacity and that of the wider public to understand digital rights and freedoms and recognise violations and undertake remedial actions.

Media (including media organizations, journalists and editors) should:

• Continue to monitor and report on as well as strongly condemn violations of online freedoms and rights.

• Seek to educate and enlighten their audiences about their rights and the importance of these rights and their roles as members of society in the exercise, enjoyment and defence of these rights.

• Provide trainings on digital security and the use of online-safety
equipment for to protect their staff and agents from unlawful surveillance or attacks.

- Facilitate increased access to information by diversifying the digital platforms on which they work and disseminate their content.
- Develop and implement robust moderation mechanisms that achieve the fine balance between the checking of online abuse or harassment and the enjoyment of the right to free expression online.
- Fact-check content they receive from citizen journalists before publication.

**General Public should:**

- Take steps to become more informed and concerned about issues of digital rights and freedoms.
- Support advocacy efforts of civil society organizations and other stakeholders.
- Mobilise as communities to influence local and national policies and legislation that relate to access to information and freedom of expression both online and offline.
- Refrain from sharing content (images, videos) that affect the sensibilities of other social media users and serve no useful purpose.
## Appendix: Incidents and key developments

<table>
<thead>
<tr>
<th>Country by country digital landscape overview</th>
<th>Digital Rights Incidents and developments in 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nigeria</strong></td>
<td>Criminalizing speech: Arrests/Detention/Sentences</td>
</tr>
<tr>
<td>- Estimated population: 190 million</td>
<td>1. <strong>January:</strong> Police arrested journalist Jerry Edoho of Ibom Nation newspaper, for sharing a post on Facebook alleging that an aircraft belonging to one of Nigeria’s airlines had crashed.</td>
</tr>
<tr>
<td>- Internet penetration: 47.7%</td>
<td>2. Police raided the offices of Premium Times, an influential news website, and arrested the Publisher, for allegedly defaming the Chief of Army staff. There was no warrant.</td>
</tr>
<tr>
<td>- Online space is regulated with laws such as the Cyber</td>
<td>3. <strong>February:</strong> Kaduna State security agents arrested and detained Audu Maikori twice for “inciting comments” following tweets alleging killings by herdsmen in Southern Kaduna.</td>
</tr>
<tr>
<td></td>
<td>4. <strong>March:</strong> Blogger Kemi Olunloyo was arrested and charged with cybercrime for sharing a post about a pastor’s alleged extra-marital affairs</td>
</tr>
<tr>
<td></td>
<td>5. The Chief Magistrate court sentenced Gambo Saeed to nine months imprisonment for defaming the governor of Katsina state</td>
</tr>
</tbody>
</table>

6. April: Austin Okai was arrested in Abuja for comments on social media deemed unacceptable by the Kogi State government.

7. Journalist, Midat Joseph of the Leadership Newspaper and Chair of the Nigerian Union of Journalists (NUJ), together with one Eusebius Yayock, were arrested WhatsApp comments deemed to be “criminal conspiracy, inciting disturbance and injurious falsehood.”

8. Police arrested social media activist, Frank Utoo, for Facebook comments deemed insulting to a prominent politician in the Kogi state.

9. Journalist Danjuma Katsina was arrested in Katsina over Facebook comments questioning legitimacy of newly elected member of Nigeria’s House of Representatives from the state. He was released following interventions from rights groups in Nigeria.

10. July: Teacher Biodun Baba was arraigned before a magistrate court in Ilorin on for allegedly insulting Senate President, Bukola Saraki on Facebook.

11. August: Johnson Musa was arrested by State Security Service operatives for posting an image of the Abuja residence of the Governor of his State on WhatsApp, with comments deemed inappropriate by the authorities.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. October</td>
<td>A student of Redeemers University was expelled for criticizing the authorities of the institution in a Facebook post.</td>
</tr>
<tr>
<td>13. January</td>
<td>Aku Obidinma, a radio broadcaster was released after 60 days in detention for Facebook posts criticizing the Imo state government.</td>
</tr>
</tbody>
</table>

**Attacks/Threats**

1. **June:** Charles Otu, of The Guardian Newspaper, was assaulted by a group of individuals in Abakaliki for critical Facebook comments about the Ebonyi state government.

**Censorship/Shutdown**

1. Nigerian government ordered the National Communications Commission (NCC) to block the domain of 21 websites. This according to the Director of Defense Information “became necessary in the light of troubling activities and misinformation capable of jeopardizing the unity of the country”.

**Surveillance**

1. Security agencies in Nigeria’s capital were also reported to have put millions of mobile phones under surveillance.
2. There was a planned launch of spy satellites with capabilities the public knows little about.
3. The Nigerian military announced monitoring of social media for inciting comments and hate speech.
<table>
<thead>
<tr>
<th></th>
<th>Engendering online rights/speech/Civil society efforts</th>
<th>Censorship/Shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Togo</strong></td>
<td>1. Civil society groups have called on government to adopt the Digital Rights and Freedom Bill to guarantee human rights online following its successful hearing at the House of Representatives</td>
<td>1. Authorities ordered a total Internet blackout during anti-government protests.</td>
</tr>
<tr>
<td>- <strong>Estimated population:</strong> 7,496,833</td>
<td></td>
<td>2. Authorities ordered a partial Internet shutdown on the eve of scheduled protests.</td>
</tr>
<tr>
<td>- Internet penetration: 7.3%:</td>
<td></td>
<td>WhatsApp and Facebook were inaccessible while other websites were rendered slow using throttling. SMS services were also disrupted.</td>
</tr>
<tr>
<td>- Poor access and high cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Government generally protects citizens’ rights to free expression and has put in place measures to improve and liberalize the telecoms sector and promote access and use.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

May: Cabinet decreed the terms for applying the Freedom of Access to Information and Public Records Law which was passed in March, 2016 to expand the freedoms of the Togolese people in accessing public information (offline and online).  
2. Local, regional and international civil society groups including the Media Foundation for West Africa denounced the shutdowns
<table>
<thead>
<tr>
<th><strong>Côte d’Ivoire</strong></th>
<th><strong>Criminalizing speech: Arrests/Detentions/Sentencing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Twenty-two percent of Cote d’Ivoire’s 23,254,184 population has access to the Internet</td>
<td>1. Several people were arrested by the cybercrime unit of the Ivorian Police Service in connection with hacking and pirating Facebook profiles for ransoms.</td>
</tr>
<tr>
<td>The national constitution guarantees of freedom of expression rights</td>
<td><strong>Online Harassment/Threats</strong></td>
</tr>
<tr>
<td></td>
<td>1. A political journalist and blogger was threatened for writing a blog in which he criticised the Ivorian Speaker of Parliament, Soro Guillaume.</td>
</tr>
<tr>
<td></td>
<td>2. An MP and Former Minister in the Ouattara government was threatened and intimidated by Police following tweets criticising the current Ivorian government.</td>
</tr>
<tr>
<td></td>
<td>3. An Ivorian singer, Josey, was trolled, mainly on Facebook for her relationship and pregnancy with an Ivorian footballer.</td>
</tr>
<tr>
<td></td>
<td>4. Nancy Ndri, a young leader who calls herself Celibbattante (single but able woman) was abused and harassed from some Internet users.</td>
</tr>
<tr>
<td></td>
<td><strong>Engendering online rights/speech/Civil society efforts</strong></td>
</tr>
<tr>
<td></td>
<td>1. <strong>May:</strong> Parliament forced by rights groups to withhold the passage of a controversial press Bill which sought to criminalize offline/online speech.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>December:</strong> Controversial press Bill which earlier sought to criminalize speech was passed with the repressive sections taken out.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ghana</th>
<th>Online Harassment/Attacks/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Population: 27.5 million</td>
<td>1. <strong>April:</strong> A Police officer made comments on Facebook thought to be disparaging of the people of the Upper West Region of Ghana.</td>
</tr>
<tr>
<td>- Internet penetration: 35%</td>
<td>2. A young lady allegedly circulated naked pictures of a Ghanaian actress. She was detained by Police.</td>
</tr>
<tr>
<td>- Among the first countries in sub-Saharan Africa to be connected to the Internet.</td>
<td>3. <strong>June:</strong> Illegal circulation of images and videos of a young military officer who was lynched by a mob in the Central Region of Ghana.</td>
</tr>
<tr>
<td>- Has liberal laws which allow for free expression online.</td>
<td>4. Two university students allegedly posted nude pictures of underage junior high school students on the Internet. They were arrested by Police.</td>
</tr>
<tr>
<td>Ghana has a Data Protection Law (2012) that protects citizens’ rights online.</td>
<td>5. <strong>August:</strong> Husband of actress Afia Schwarzenegger recorded and circulated a video that captures her nakedness. He was arrested and charged.</td>
</tr>
<tr>
<td></td>
<td>6. An 18-year-old Rashida Mohammed, allegedly posted a nude video of herself on social media. She was invited for questioning by the Police.</td>
</tr>
<tr>
<td></td>
<td>7. Two persons allegedly circulated nude pictures of a 20-year old former student of the Yilo-Krobo Senior High School. They were arrested by the Somanya District Police Command.</td>
</tr>
</tbody>
</table>

### The Gambia

- Internet penetration is estimated at 17 percent.
- Mobile phone penetration is well over 100 percent with four main cell phone companies.
- Mobile phone penetration is well over 100 percent with four main cell phone companies.
- Freedom of expression has significantly improved under the Adama Barrow regime with most blocked websites and apps under the Jammeh regime becoming accessible. Nonetheless, Internet freedom remains at risk as many draconian laws of the former regime remain.

### Criminalizing speech: Arrests/Detentions/Sentencing

1. Fatou Badjie, was arrested for allegedly insulting the new president,
2. Four soldiers were arrested for being part of a WhatsApp chat group allegedly engaged mutinous acts.
3. **July:** Lance Coporal Samboujang Bojang was detained by Military Police for comments deemed mutinous. He was later hospitalized after alleged torture.
4. **August:** Kebebe a youth activist summoned for questioning by the Youth and Sports Minister for criticising him
5. **Oct:** Fatou Manneh was fined D10,000 ($200) in default to serve a prison term of one year for criminal libel, false publication and broadcasting. The accused, Fatou Manneh, had disseminated naked pictures of the complainant on WhatsApp.

### Engendering online rights/speech/ Civil Society Efforts

1. **June:** Sedition was declared unconstitutional

---

- http://thepoint.gm/africa/gambia/article/woman-gets-heavy-fine-for-false-publication
Liberia

- Internet penetration: 8% with services provided mainly by MTN-Lone Star; Cellcom (Now Orange) and Libtelco

- Despite improvements, statutes remain that criminalize speech (online and offline) offenses

- Civil society continues to advocate for the repeal of such laws

No digital rights violation was recorded in Liberia in 2017. However, various incidents that occurred in the country affected Internet use and access in Liberia. While there was no report of government actions to disrupt the country’s digital space, there were efforts by private groups to block citizens from expressing themselves online as the examples below show:

Censorship/Shutdown
1. Administrators of several sites and social media groups blocked people from accessing the platforms accusing the victims of using vulgar language.
2. The Costa Show on Shaita FM which also streams live was known for blocking callers who expressed contrary views.
3. Blocking was also prevalent on the Darius Dillon Forum on Facebook
4. Two Pro-George Weah FM stations also blocked listeners who critiqued him during the electioneering period.
5. Pro Joseph Boakai Radio Monrovia blocked some listeners

Cyber attacks
1. Britain’s National Crime Agency (NCA) arrested suspect accused of the November 2016 hacking of Internet services
### Zimbabwe

**Mobile Internet makes up most of the Internet access in Zimbabwe**

Most Internet traffic targets social media applications, Facebook and Whatsapp.

including the Mirai malware on Liberia Internet services. The suspect, Daniel K., reportedly told the court that a Liberian Internet service provider (ISP) paid him $10,000 to carry out the attack against its competitors and sick man.”

**Criminalizing speech: Arrests/ Detentions/Sentencing**

1. **January:** Prominent pastor and leader of the #thisflag movement, Pastor Evan Mawarire was arrested and accused of breaching the Criminal and Codification Act in his efforts to ‘subvert a democratically elected government’.
2. **September:** Pastor Evan Mawarire was again arrested after he published a video recording which was largely viewed as critical of the government.
3. **November:** Martha O’Donovan, a journalist from the United States working with creative hub, Moto republik was arrested for a tweet that was deemed insulting to former president Mugabe. The tweet suggested that Mugabe relied on a catheter for survival “We are being led by a selfish man
4. Citizen journalists from Busstop TV a local blogging channel were expelled from a Zanu PF rally after they circulated a video on Facebook that confirmed earlier

---

- [http://www.sundaymail.co.zw/president-clarifies-chinamasas-ministry/](http://www.sundaymail.co.zw/president-clarifies-chinamasas-ministry/)
Since the adoption of a new Constitution in 2013, civil society has called for the alignment of the existing laws with the constitution which provides a more expansive bill of rights.

Section 61 of Zimbabwe’s constitution recognizes the right to freedom of expression and freedom of the media.

Despite these provisions the Zimbabwean government relies on unconstitutional laws to discourage and suppress online freedoms.

<table>
<thead>
<tr>
<th>Censorship/Shutdown/Threats/Intimidations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>May:</strong> The Movement for Democratic Change (MDC-T) reportedly informed its members that it would not address grievances (on the formation of a coalition) that were shared on social media.</td>
</tr>
<tr>
<td>2. <strong>June:</strong> Zanu PF banned its members from bringing cellphones to its politburo meetings in order to curb leaks to the media.</td>
</tr>
<tr>
<td>3. Deputy Minister of Media Information and Broadcasting Services Thokozile Mathuthu was reported to have said that the government would ‘curb the abuse of social media.</td>
</tr>
<tr>
<td>4. <strong>October:</strong> Prior to his resignation, former President Robert Mugabe, introduced a new ministry, the Cybersecurity, Threat Detection and Mitigation to ‘weed out’ those bent on abusing the Internet for sinister agendas. This prompted an increase in self-censorship among online users (especially on Whatsapp groups as evidenced by memes and a spoof government notice) as there was uncertainty on the role of the ministry.</td>
</tr>
<tr>
<td>5. There was also an emerging trend elections. The government has instituted</td>
</tr>
</tbody>
</table>

- [The African Declaration on Internet Rights and Principles: http://africanInterne\ ights.org/](http://africanInterne\ights.org/)
Digital rights awareness and observance is generally low in Zimbabwe given strict control of dissenting opinion by the Mugabe government. As a result African civil society organisations have coalesced to work to increase awareness on digital rights through the African Declaration on Internet Rights and Freedoms.

<table>
<thead>
<tr>
<th>Surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. There were concerns raised about the equipment at the new National Data Centres which were sourced from China, raising questions on the security of the data stored in these centres. The concerns were premised on recent stories of Chinese spying on the African Union headquarters.</td>
</tr>
</tbody>
</table>

**Engendering online rights/speech/ Civil Society Efforts**

1. **January:** There was a citizens’ uproar on over 2500 percent hike of mobile data. Citizens took to social media in a #datamustfall campaign.
2. Despite calls in May by stakeholders for a fair and competitive pricing policy on landing bandwidth, and a commitment by Minister Mandiwanzira, the year ended without it.
3. Mobile Network Operators (MNOs) continue to have special subsidised data bundles for their subscribers, a move that

- [https://qz.com/1192493/china-spied-on-african-union-headquarters-for-five-years/]
has significantly reduced the utilitarian value of the Internet for Zimbabweans.

4. Government maintains significant control over the networks, following the US$40 million takeover of Telecel Zimbabwe through its Internet Service Provider, Zarnet

5. Econet remains dominant telecom player but there was a significant increase in subscribers of government owned Netone during the #datamustfall protest against service providers that had increased prices.

6. March: Telone launched it’s data centre, which is expected to develop into the National Data Centre which is provided for in Zimbabwe’s 2016 National Policy for Information Communications Technology. Concerns around this include the fact that Zimbabwe does not have a singular Data Protection law. Provisions for data protection are scattered across several Acts and were expected to be amended in the Data Protection Bill which remains to be gazetted into an Act.

7. A series of digital rights awareness meetings by MISA Zimbabwe across metropolitan provinces (Harare, Bulawayo, rural Midlands, Manicaland, Masvingo, Matabeleland etc) exposed fears among the citizenry for interacting and sharing on political developments in the country.

8. Civil groups continue to be concerned about the lack of awareness by the
majority of online uses on their rights to the privacy and their ability to secure their communication from possible violation. 

Surveys by the Digital Society of Zimbabwe revealed that digital security is not standard practise.

9. Feminists, gender and sexual minority groups in Zimbabwe argue that the Internet, for them, is not a ‘technology of freedom’ as they continue to face violence on line. They expressed these during a meeting hosted by the Association for Progressive Communications (APC) on the Feminist Principles on the Internet (FPIs).

Coercive posture towards online free expression

1. April: Zanu PF politician Psychology Maziwisa asserted that the youth’s use of social media to engage in political debates was ‘unpatriotic’.

2. May: On World Press Freedom Day, the Chairperson of the Parliamentary Portfolio Committee on Information and Communication Technology, Nelson Chamisa, was reported to have said there was no point discussing digital rights when the majority of the population has no acces.

3. July: Minister of Media Information and Broadcasting Service, Chris Mushowe castigated politicians who ‘fight’ political battles on social media saying they were ‘abusing their right to freedom of expression’.

- https://www.dailynews.co.zw/articles/2017/10/14/ministers-blames-social-media-for-panic-buying/
4. **October:** Minister of Industry and Economic Development, Mike Bimha said that a ministerial taskforce to investigate price hikes and panic buying in the country found social media to be the cause.

5. **November:** Phillip Valerio Sibanda, then commander of the Zimbabwe National Army said that social media was a threat’ to culture.

6. **December:** After Robert Mugabe’s resignation, the Zimbabwe Defence Forces issued a statement warning against the “abuse of social media”.

**Hacking**

1. A report by an American software company, Rapid LLC, ranked Zimbabwe as the most hackable country out of 183 countries. According to the 2017 National Exposure Index many Internet protocol (IP) addresses in the country still use outdated protocol leaving them susceptible to cyber-attacks.

2. **August:** Minister of Information, Communication Technology, Postal and Courier Services, Supa Mandiwanzira confirmed that about two banks had been affected by ransomware cryptoworm virus, WannaCry, after hackers instituted it in May 2017.

3. **June:** Students took to social media on hacking of the National University of Science and Technology (NUST) and

the Harare Institute of Technology (HIT) websites by hackers demanding more than $6 billion to restore information to their websites. While HIT officials confirmed the attack, officials at NUST denied theirs, despite insistence by both lecturers and students that they had been unable to access the site on the day of the attack”.

<table>
<thead>
<tr>
<th>Cameroon</th>
<th>Criminalizing speech: Arrest/Detention/Sentencing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Prior to Internet shutdowns in response to protests in Anglophone regions, the Communications ministry sent text messages to mobile phone subscribers, notifying them of penalties, including long jail terms and excessive fines, for “spreading false news” via social media</td>
</tr>
<tr>
<td></td>
<td>2. Journalists, activists, ordinary citizens were arrested for criticising government officials or commenting about the Anglophone crises on social media.</td>
</tr>
<tr>
<td></td>
<td>3. The co-founder of Camer Veritas online magazine accused of inciting terrorism was arrested and detained.</td>
</tr>
<tr>
<td></td>
<td>4. A US-based Cameroonian writer and scholar, Nganang, was arrested on December 6, 2017 at the airport in Douala for publishing an article in Jeune Afrique news magazine concerning the political repression and crackdown on citizens of Anglophone Cameroon by the government. Nganang was also accused by the government of insulting constitutional bodies and</td>
</tr>
</tbody>
</table>

inciting violence on a Facebook post allegedly written after he visited the Anglophone regions. He was freed on December 27 (three weeks after his arrest) and deported to the US and banned from ever coming back to Cameroon

**Censorship/Shutdown**

1. **January:** On the eve of scheduled protests in the two Anglophone regions, The Ministry of Post and Telecommunication shut down Internet connection in English Speaking Cameroon. The Communication minister and government spokesman, Issa Tchiroma Bakary, indicated the shutdown was a result of the propagation of false information on social media capable of inciting hate and violence in the crisis-hit regions. The Internet shutdown lasted 94 days, making it one of the longest Internet blackouts to be recorded in Africa. According to Access Now, a civil society organization promoting digital rights, the shutdown that deprived about 7 million citizens of access to information, resulted in the loss of about U.S. $4.5 million in a country with a per capita income of about $1,200. The Internet shutdown also had serious repercussions on personal, economic and social lives of the Anglophone people as businesses that required the Internet were forced to shut down. It was a particular blow for Cameroon’s “Silicon Moun

- https://www.accessnow.org/victory-cameroon-94-days-Internet-back/
2. **October:** The Paul Biya led administration again shut down the Internet ahead of protests against political and economic discrimination in the English-speaking regions. The shutdown lasted about 150 days. Cameroon is yet to recover from the economic losses the two Internet blackouts have caused.

## Coercive posture towards online free expression

1. Prior to Internet shutdowns in response to protests in Anglophone regions, the Communications ministry warned social media users against the spreading of information.

### Coercive posture towards online free expression

<table>
<thead>
<tr>
<th>DR Congo</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminalizing speech: Arrests/Detention/Sentencing</strong></td>
</tr>
<tr>
<td>1. Defamation and libel laws were used to harass journalists and activists in the country. Government repression offline has been extended to the online space.</td>
</tr>
<tr>
<td><strong>Censorship/Shutdown</strong></td>
</tr>
<tr>
<td>1. <strong>August:</strong> Authorities ordered Internet</td>
</tr>
</tbody>
</table>
Constitution provides for free speech Government cracked down on protests against President Joseph Kabila tenure extension.

- Constitution provides for free speech Government cracked down on protests against President Joseph Kabila tenure extension.

- Government instructed service providers to slow down Internet connection to make it difficult for the transmission of images on social media platforms. Oscar Manikunda Musata, the Post and Telecommunications Chief Regulator, instructed the General Director of mobile network Orange DRC to take preventative measures to reduce the capacity to transmit “abusive messages.”

2. **December:** Government authorized a complete nationwide Internet shutdown and disruption of SMS services a day before scheduled protests by activists of the country’s Catholic Church.

Uganda

- Uganda has a population of about 39 million (2015) with 31% Internet penetration

- Fast growing sector due to increased use of mobile telephony.

- Freedom of the press, expression and information are guaranteed in the 1995 Ugandan Constitution

Criminalizing speech: Arrests/Detention/Sentencing

1. **September:** The Uganda Communications Commission (UCC) warned social media users that it was illegal to share receive or post information on the constitutional age-limit debate which was on-going at the time. This followed the decision by the party leadership to remove the presidential age limit. The UCC threatened to prosecute anyone found guilty.

2. **April:** Stella Nyanzi, a human rights activist was accused of cyber harassment against the President, Museveni for criticising the President and his wife over an unfulfilled promise to distribute sanitary pads to school girls to curb dropping out
The Ugandan government has also adopted different laws and policies to govern Internet freedom, and ratified regional and international frameworks that guarantee the respect for freedom of expression,

However, sections of these laws are equally used to silence or punish citizens for enjoying their rights online.

3. Twenty-six persons were arrested and charged for offensive communication and cyber harassment under various laws:
   - Thirteen journalists
   - Four artists
   - Two political activists
   - Six officers of the Ugandan People’s Defence Forces (UPDF)
   - One academic

4. May: VJ Junior (famous movie translator) and his colleague were charged for cyber harassment and offensive communication for posts they made on a WhatsApp group about the Uganda Film Producers Association.

5. October: Journalists Stanley and Robert Ndawula were arrested and accused of malicious publications for publishing stories about the Police Force’s image on the online news agency The Investigator.

Physical Attacks/Threats
1. Gertrude Uwitare of NTV Uganda was beaten by unknown assailants after posting a message on her blog supporting comments by human rights activist Stella Nyanzi criticizing President Museveni
2. A journalist from NTV Uganda was kidnapped.

Censorship/Shutdowns
1. May: following an expansion of his powers, communications minister ordered
*Social media users often create pseudonyms to protect their anonymity online*

Blogging is still highly used by the youth to discuss controversial issues

---

the Uganda Communications Commission (UCC) to switch off all unchecked SIM cards in spite of a Parliamentary motion to extend the deadline for SIM card re-registration.

**Surveillance**

1. **June:** The media regulatory body, Uganda Media Centre, indicated publicly that a new social media monitoring unit was set up to scan for critical posts made on social media.

2. **July:** Daily Monitor newspaper reported that the Ugandan Government was in contact with the Chinese government to build the “technical capacity to monitor and prevent social media abuse”. The act was premised on the Regulation of Interception of Communication (RIC) 2010 which empowers the government to conduct real-time electronic surveillance of persons suspected of terrorism and to interfere with personal communications for reasons of national security.

3. **April:** Parliament passed a new bill (Uganda Communications Amendment Bill) removing the checks and balances on the minister’s supervision of the communication sector.

**Coercive posture towards online free expression**

1. **May:** The Minister of Information,
Communication & Technology (ICT) and National Guidance remarked that there was the need for the Ugandan government to “filter social media content that the public posts on Facebook, WhatsApp and Twitter” to restrain abusive speech online.

<table>
<thead>
<tr>
<th>Ethiopia</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet penetration of 15%</strong></td>
</tr>
<tr>
<td><strong>Poor infrastructure and government monopoly of telecoms sector.</strong></td>
</tr>
<tr>
<td><strong>Data cost is very expensive for the ordinary people.</strong></td>
</tr>
</tbody>
</table>

**Tense freedom of expression landscape amidst government accusations that social media activists spread inciting messages.**

<table>
<thead>
<tr>
<th><strong>Criminalizing Speech: Arrests/Detentions/Sentencing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>May:</strong> Prominent opposition activist, Yonatan Tesfaye, was sentenced to six and a half years on terrorism charges based on Facebook posts criticizing government’s handling of the Oromia protests.</td>
</tr>
<tr>
<td>2. <strong>May:</strong> Editor-in-chief of opposition outlet Negere Ethiopia, Getachew Shiferaw, was sentenced to one and a half years in prison on subversion charges for Facebook comments in support of exiled journalist.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Censorship/Shutdown</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>May:</strong> Authorities shut down the Internet, for 12 hours, ahead of a scheduled national examination ostensibly to prevent exam leakage.</td>
</tr>
<tr>
<td>2. <strong>December:</strong> Government restricted access to social media in the wake of renewed clashes that had led to deaths in the Oromia region.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Engendering online rights/speech/ Civil Society Efforts</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The government in August this year lifted a state of emergency imposed in October 2016 to quell similar protests in the Oromia and Amhara regions.</td>
</tr>
</tbody>
</table>

Somalia

- Estimated population is 14.32 million (2016) with 1.7% Internet penetration

Following years of civil war, Somalia’s entire telecoms sector collapsed.

- Somalia now has some of the most technologically advanced and competitively priced telecoms services in the world.

Criminalizing Speech: Arrests/Detentions/Sentencing

1. July: Somalia’s Council of Ministers adopted a repressive new media law which sought to stifle freedom of expression rights both offline and online in the country.

1. Police arrested a journalist with Horseed Media news website following a Facebook post alleging the involvement of Puntland President Abdiweli Mohamed Ali in a counterfeit money-printing scam.

Censorship/Shutdown

1. Courts in Somaliland, a self-declared republic in north-western Somalia, were responsible for blocking five news websites.

2. January: two telecom companies, SOMCABLE and SOMTEL blocked access to popular news websites, Aftahannews.com and Hubaalmedia.com, in Somaliland.

3. SOMCABLE also blocked access to another popular news website Hadhwanagnews.com for publishing critical content about the firm.


55
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. July</td>
<td>Mogadishu Authorities banned SMS services widely used by radio stations to disseminate news articles via text messages. This followed threats to Hormuud Telecom, the largest company providing the service by Al-Shabaab extremists.</td>
</tr>
<tr>
<td>6. November</td>
<td>During presidential elections, Somaliland Electoral Commission directed telecommunications companies to block over a dozen social media platforms including Facebook, Twitter, WhatsApp, Snapchat, Viber and Instagram in order to limit “hate speech”, “misrepresentation of election results” and “fake news”</td>
</tr>
</tbody>
</table>

**Engendering online rights/speech/ Civil Society Efforts**

1. **August**: The Federal parliament of Somalia passed a National Communication Act that will help government increase revenue from the country’s telecommunication sector and tackle the growing rate of cybercrimes in the country.