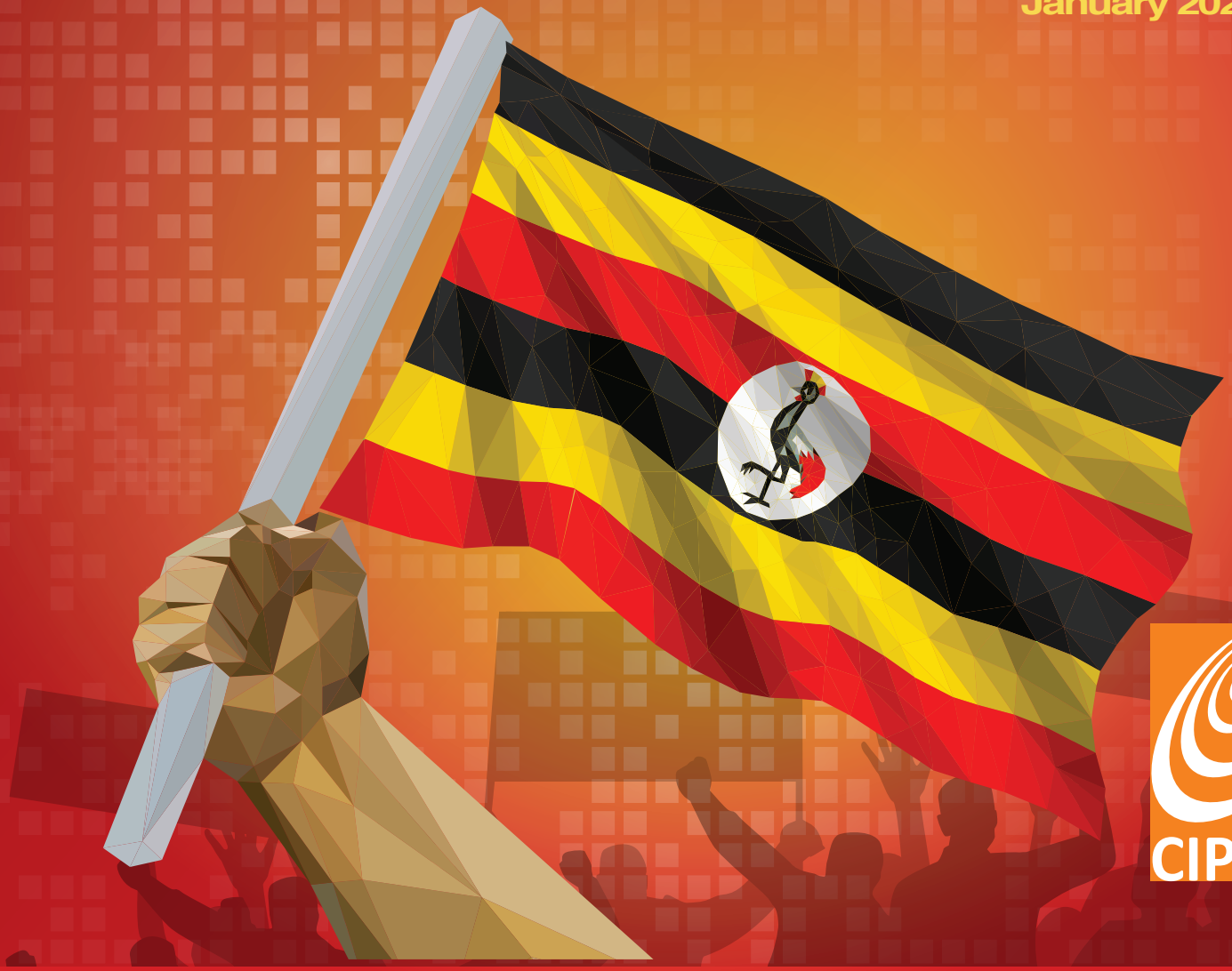
State of Internet Freedom in Uganda 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020



CIPESA

Table of Contents

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Uganda tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Bostwana, Burundi, Cameroon, Chad, the DRC, Ethiopia, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Daniel Mwesigwa as the main content contributor to this report.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Uganda 2019
Published by CIPESA,
www.cipesa.org
January 2020

1 Introduction

1.1 Introduction

By 2000, about 25,000 Ugandans out of the then population of 21.6 million were estimated to be connected to the internet.[1] While the market for telecommunications services was undergoing major reforms to pave way for full liberalisation, the internet's significance in civic and democratic processes was limited to elite sections of academia, civil society, business, government and international development.[2] At the time, Uganda's telecommunications liberalisation policy was considered one of the most progressive and inclusive in sub-Saharan Africa.[3]

In 2002, the government passed the Anti-Terrorism Act to curb the growing wave of terrorist activities in Uganda and neighbouring countries. Uganda had suffered instability caused by the Lord's Resistance Army (LRA) guerrilla war in northern Uganda since 1987, and the Allied Democratic Forces (ADF) insurgency in western Uganda since 1996.[4] At the height of the insurgencies, the anti-terrorism law gave government powers to surveil and intercept communications of persons suspected to be planning or involved in acts of terrorism.[5] During this period, there were little to no cases of internet freedom violations reported.

However, the period between 2005 and 2010 became determinative of the shape of internet freedoms and wider freedom of expression in Uganda. In 2005, the presidential two-term limit was lifted, allowing President Yoweri Museveni to contest for a third term in the 2006 general elections, which he won. The period was also characterised by politically charged protests and high-handed responses from the state. In September 2009, the central government blocked a popular cultural leader from Buganda kingdom – Uganda's largest ethnic group – from visiting one of their constituencies in Kayunga district, central Uganda,[6] leading to violent riots that resulted in loss of lives.[7] The government responded by ordering the closure of four radio stations and detaining a talk-show host, Robert Kalundi, and suspending open-air talk-shows, commonly known as ebimeeza, accusing them of "inciting the riots."[8]

1 *ITU, The Internet Case in an African LDC: Uganda Case Study," January, 2001, ailable at https://www.itu.int/ITU-D/ict/cs/uganda/material/uganda.pdf*
2 *Ibid.*
3 *Charles Byaruhanga, Managing Investment Climate Reform: Case Study of Uganda Telecommunications, 2004, http://siteresources.worldbank.org/INTWDRS/Resources/477365-1327693758977/8397896-1327771331430/byaruhanga_uganda_telecoms.pdf*
4 *The New Humanitarian, Uganda: LRA, ADF on American terrorist list," December 07, 2001, https://reliefweb.int/report/democratic-republic-congo/uganda-lra-adf-american-terrorist-list*
5 *Available at https://www.icj.org/wp-content/uploads/2012/04/icj_anti-terrorism_act_position_paper_2002.pdf*
6 *Katikiro Walusimbi Blocked from proceeding to Kayunga, https://ugandaradionetwork.com/story/katikiro-walusimbi-blocked-from-proceeding-to-kayunga*
7 *Uganda riots enter second day, https://www.aljazeera.com/news/africa/2009/09/200991191146684575.html*
8 *Four radio stations closed and a talk-show host detained for "inciting riots", https://rsf.org/en/news/four-radio-stations-closed-and-talk-show-host-detained-inciting-riots*

Between 2010 and 2015, the political environment in the post-2011 election was similarly ripe for protests. This period experienced more domestic political contestations and geopolitical shifts of information control and power. The Arab Spring, a series of anti-government protests and insurgencies, started in December 2010 in Tunisia and swept across seven countries in the Middle East and North Africa.[9] Through 2011, autocratic leaders in Tunisia, Egypt, Libya, and Algeria were deposed through sustained street protests and armed conflicts. The unrest in North Africa was fuelled through evocative commentary and coordination through social media and other digital communication channels.

In the same year, 2011, the Uganda government instructed mobile network operators to block Twitter and Facebook in the heat of "Walk to Work" protests.[10] In 2011, the Parliament enacted cyber-related laws, namely the Computer Misuse Act, the Electronic Transactions Act, and the Electronic Signatures Act, to protect and regulate use of electronic and computer systems. Later in 2013, the government passed the Public Order Management Act to regulate public assemblies.

In 2012, the Uganda Communications Commission (UCC) kickstarted SIM card registration under the Regulation of Interception of Communications Act (2010) which provides for registration of existing SIM cards.[11] The UCC justified the process as necessary to "help law enforcement agencies to identify the mobile phone SIM card owners", "track criminals who use phones for illegal activities", "curb other negative incidents such as; loss of phone through theft, nuisance/hate text messages, fraud, threats and inciting violence", and "help service providers (network operators) know their customers better."[12] Without sufficient constitutional guarantees on data protection and privacy, the move raised concerns of mass surveillance and was seen as a threat to fundamental rights such as privacy.[13]

The government is reported to have procured FinFisher, an intrusion and surveillance software that was purportedly used in an operation code named "Fungua Macho" in early 2012.[14] Meanwhile, in 2013, Edward Snowden, a former United States intelligence and defence contractor, revealed that the National Security Agency (NSA) was intercepting and surveilling global communication channels to track and profile citizens without their knowledge through NSA's so-called 'five eyes' surveillance partnership with security agencies in the United Kingdom, Canada, Australia, and New Zealand.[15] This set the stage for the bolder policy and technical approaches on internet control and the attendant internet freedoms in Uganda. Leaked emails from a 2015 WikiLeaks archive showed that the Uganda government was actively looking to procure more technology from Italian Hacking Team and German-based Gamma GmbH to strengthen its surveillance capacities.[16]

9 Erin Blakemore, What was the Arab Spring and how did it spread?, March 19, 2019, https://www.nationalgeographic.com/culture/topics/reference/arab-spring-cause/

10 ACME, "In face of unrest, Uganda seeks to block social media websites," April 19, 2011, available at https://acme-ug.org/2011/04/19/in-face-of-unrest-uganda-seeks-to-block-social-media-websites/

11 See http://web.archive.org/web/20131201000000/https://www.ucc.co.ug/data/smenu/23/SIM-Card-Registration.html*

12 Ibid.

13 Edrine Wanyama, The Stampede for SIM Card Registration: A Major Question for Africa," April 18, 2018, https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/

14 Privacy International, "Ugandan Government Deployed FinFisher Spyware To 'Crush' Opposition, Track Elected Officials And Media In Secret Operation During Post-Election Protests, Documents Reveal," October 15, 2015, available at https://tinyurl.com/y7dxulru

15 James Ball, et. al., Revealed: how US and UK spy agencies defeat internet privacy and security, September 06, 2013, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

16 Daniel Mwesigwa,"Leaked Emails: How Hacking Team and Uganda government want to spy on you, July 22, 2015,https://www.dignited.com/14494/leaked-emails-how-hacking-team-and-uganda-government-want-to-spy-on-you/

From 2015 to 2019, Uganda experienced its first internet shutdown. During the February 2016 presidential election, access to social media and mobile money was shut down for more than 24 hours over undefined 'national security' concerns. Again in May that year, access to social media was blocked during the presidential swearing-in ceremony.[17] Two years later, President Museveni accused social media users of using the internet to spread "lies and falsehoods", and instructed the finance ministry to levy a tax on usage of Over The Top (OTT) services.[18] The president also cited the need for the country to grow its national tax revenues. Also, in 2018, the government installed the "Intelligent Network Monitoring Verification System" (INMS) which has access to mobile network operators' traffic in order to track and verify transaction details including voice and data.[19]

The various developments explored above led to a regression in internet freedom in Uganda over the last decades, with affronts to freedom of expression and association, right to information, and privacy, among others.

1.2 Aim of the Study

This study sought to document the extent to which government controls of the digital space have affected or limited internet freedom in Uganda over the last 20 years. Specifically, the study traced the trends and developments in the digital space in the period between 1999 and 2019. The study focused on the proliferation of retrogressive or repressive policies and laws; surveillance and surveillance capacity of the government; digitalisation programmes; censorship; and the new frontiers like the introduction of internet-related taxes. The study also sought to identify and recommend measures that different stakeholders – the governments civil society, technology companies, academia, and the media - can take to secure internet freedom in Uganda.

17 Social Media Blocked in Uganda Ahead of President Museveni's Inauguration, https://advox.globalvoices.org/2016/05/11/social-media-blocked-in-uganda-ahead-of-president-musevenis-inauguration/

18 Elias Biryabarema, "Uganda leader says social media used for 'lying', defends tax for access," July 4, 2018, available at https://www.reuters.com/article/us-uganda-internet/uganda-leader-says-social-media-used-for-lying-defends-tax-for-access-idUSKBN1JU2NV

19 Uganda regulator sets up system to track daily telco revenues, social media tax." July 04, 2018, https://www.theeastafrican.co.ke/business/Uganda-installs-system-to-track-telco-revenues/2560-4646012-xnnij7/index.html

2 Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Literature review included various reports of previous studies, media reports, academic works, and government documents. The legal and policy analysis included a review of relevant laws, policies, proposed legislation, regulations, directives, case law and procedures and practices in the country. The review provided an understanding of the trend of government internet controls over the last two decades.

The key informant interviews were conducted with staff of private companies (such as banks, telecoms firms, Internet Service Providers), government ministries (such as those responsible for ICT, security), semi-autonomous bodies such as electoral commissions and telecoms regulators, media houses, social media users, human rights defenders and activists, consumers' associations, academics and lawyers.

3 Country Context

3.1 ICT Status

Over the last 20 years, there has been exponential global growth of mobile telephony services coupled with dwindling costs of devices and internet bandwidth, and a favourable political and business environment for private sector investments.[20] Between 2010 and 2014, the number of mobile broadband subscriptions in Uganda grew by approximately 70% per year, the highest stretch of growth in the last 20 years.[21] In contrast, the fixed broadband penetration rate has remained below 1%. According to the UCC Communications Sector Performance Report (September 2019), Uganda has 15.2 million internet subscriptions, representing a 37.9% internet penetration rate.[22] About 99% of the internet subscriptions are based on mobile telephony. According to the GSMA, a global mobile operators' association, over 98% of Uganda's population is covered by 2G, 78% by 3G, and 23% by 4G.[23]

Uganda has 33 Public Service Provider (PSP) license operators, that is, mobile operators licensed to sell voice and data services; and 22 Public Infrastructure Provider (PIP) licensees, namely the providers allowed to establish and operate communication infrastructure. Mobile voice services continue to dominate the telecommunications sector, with four main providers – MTN, Airtel, Africell, and UTL. However, the market is highly concentrated with MTN Uganda and Airtel Uganda collectively controlling more than 84% of the market.[24] Further, Uganda's data costs are higher than those in most neighbouring countries. For example, 1 GB of data costs up to 16.2% of an average Ugandan's monthly income compared to the sub-Saharan average of 9.3%.[25] Mainstream internet adoption in the country remains low due to structural bottlenecks such as lack of digital skills and literacy, gender disparities, and affordability.[26] These bottlenecks have significantly inhibited internet freedom as the majority of citizens remain unconnected, and for those who are, the digital divide inhibits the full enjoyment of the internet for its potential social, economic, and political benefits.

20 Charles Byaruhanga, Managing Investment Climate Reform: Case Study of Uganda Telecommunications, 2004,http://siteresources.worldbank.org/INTWDRS/Resources/477365-1327693758977/8397896-1327771331430/byaruhanga_uganda_telecoms.pdf

21 Rachel Alemu. The Liberalisation of the Telecommunications Sector in Sub-Saharan Africa and Fostering Competition in Telecommunications Services Markets: An Analysis of the Regulatory Framework in Uganda. Vol. 6. Springer, 2018.

22 See https://uccinfo.blog/2020/01/30/communication-sector-report-september-2019/

23 See https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Connected_Society_Uganda_Overview.pdf

24 See https://www.statista.com/statistics/671666/mobile-subscription-share-in-uganda-by-operator/

25 See https://a4ai.org/affordability-report/data/?_year=2018&indicator=INDEX&country=UGA

26 See https://uccinfo.blog/2020/01/30/communication-sector-report-september-2019/

3.2 Political Environment

Uganda is a landlocked country in East Africa bordering Kenya to the east, Tanzania in the south, the Democratic Republic of the Congo in the west and South Sudan in the north. Uganda's population has steadily grown from 22.9 million in the year 2000 to over 40 million by 2019. About 80% of Ugandans live in rural areas. Kampala has a population of 1,659,600 compared to the next largest urban centre at 365,000 people.[27] The country has had a long reign of relative peace and stability in the last two decades. Over time, the country has registered considerable socio-economic growth. However, corruption is rampant, including in senior levels of government and hinders meaningful delivery of social services. Uganda's president, Yoweri Museveni, has been in power for 33 years, and is routinely accused of harassing and brutalising political dissenters, and of rigging elections. His government has expunged presidential term limits and age limits to enable him to continue running for office. The media are regularly attacked by government officials, including the police, and human rights organisations are also often the subject of attacks by state and non-state actors. From 2010 the country has enacted numerous legislations to regulate the use of digital space. The laws largely impact negatively on the exercise of digital freedoms.

3.3 Economic Status

As of 2018, Uganda ranked 162 out of 189 countries on the United Nations Development Programme (UNDP) Human Development Index (HDI), which is "a summary measure of average achievement in key dimensions of human development". This places it among the worst performing countries. Uganda has a gross domestic product (GDP) per capita of USD 604, according to the World Bank.[28] The economy grew at an average rate of 6.9% between 1990 and 2012.[29] However, average growth fell below 5% between 2013 and 2017 as the country grappled with private sector credit constraints, poor harvests due to adverse weather, unrest in South Sudan, and underperformance in public sector project execution.[30]

According to the Center for International Development, Uganda is projected to become one of the fastest growing economies in the world, averaging seven percent annual rates by 2027.[31] Over 69% of the working population are employed in the agriculture sector, which contributes 25% to the GDP.[32]

27 *Uganda Population. (2019-08-28). Retrieved 2019-10-03, from http://worldpopulationreview.com/countries/uganda/*
28 *Seet https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UG*
29 *See https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2018&locations=UG&start=1983&view=chart*
30 *Ibid.*
31 *See http://atlas.cid.harvard.edu/growth-projections*
32 *See https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS?locations=UG ; https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS?locations=UG*

4 Results

4.1 Key Trends of Internet Control Over the Last Two Decades

This section traces the history and evolution of internet control measures adopted by the Government of Uganda, from 1999 to 2019. It also attempts to provide an understanding of the social, political and socio-economic considerations behind these control measures.

4.1.1 Weaponising the Law to Legitimise Actions

In Uganda, some ICT-related laws contain provisions that infringe on digital rights. During the period between 1999 and 2019, the provisions have become more restrictive, including providing for state surveillance, interception of private communication and the introduction of online censorship.

Legalising Surveillance and Interception of Communication

During the study period, the government adopted various legislation to legitimise surveillance practices through legalised interception by state agencies supported by communication intermediaries. In 2010, Uganda enacted the Regulation of Interception of Communications Act (RICA), 2010 which provides for lawful interception and the monitoring of communications through telecommunication, postal or any other related service or system. The law buttressed section 19 of the Anti-Terrorism Act of 2002 which also permits interception of communications.

Further, section 3 of RICA provides for the establishment of a monitoring centre overseen by the minister for communication. Section 11 of the Act requires service providers to, always, technically assist the government to intercept communications by installing hardware and software to enable the interception of communications or when required. A failure to comply with the requirement attracts a fine of UGX 2,040,000 (USD 583) or imprisonment for a period not exceeding five years, or both; and a possible cancelation of the provider's license. This law restricts the privacy of communications as well as the security of personal data. Further, it has the potential to cause self-censorship owing to fears of communication being intercepted.

Rise of National Security and Fighting Terrorism as Justification for Repressive Laws

The protection of national security, preservation of public order and the fight against terrorism have been used in Uganda to enact repressive legislation. Moreover, these terms have not been clearly defined and therefore are largely ambiguous. In turn, they have been abused by state agencies.

Under RICA, interception is deemed lawful where a warrant to do so is issued by a judge if there are "reasonable grounds" for interception to take place. Lawful grounds include "an actual threat to national security or any compelling national economic interest" or "concerning a potential threat to public safety or national security" and "national interest involving the State's international relations or obligations".[33] National security measures may aid government control of the nation, promote peace and remove unnecessary fear from the citizens of the country. However, where misapplied, they could have a chilling effect on human rights, including freedom of expression and freedom of information.

On the other hand, the Anti-Terrorism Act of 2002[34] permits the interception of communications to be conducted on grounds such as safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism. Amendments to the Act were made in 2017 to include broad criminalisation of terrorism to include "indirect" involvement in terrorist activities and the "'unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature."[35]

Silencing Dissent and Criticism through Criminalising Free Speech

The systematic use of criminal law to prosecute and punish government critics has become a trend in different countries, including Uganda.

Enforcing Insult Laws

A key trend has been the use of "insult laws". Section 24 of the Computer Misuse Act 2011 criminalises cyber harassment, while section 25 prohibits "offensive communication". These two provisions have been used to arrest and charge government critics for their online activities. In May 2016, Henry Mutyaba and Robert Darius Tweyambe were arrested for allegedly circulating a photo on Facebook suggesting that Museveni was dead. The duo was charged with demeaning the person of the president and charged under the Computer Misuse Act. In December 2016, Swaibu Nsamba Gwogyolonga, a political activist and government critic, was arrested and charged with offensive communication for publishing on his Facebook account a photoshopped image of President Museveni lying dead in a coffin.[36]

33 The Anti-terrorism Act No.14 of 2002, "http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf

34 The Anti-terrorism Act No.14 of 2002, http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf

35 Anti-Terrorism Amendment Act 2017 https://ulii.org/ug/legislation/act/2017/4

36 FDC chairperson arrested over posting Museveni in coffin on Facebook, https://www.monitor.co.ug/News/National/FDC-chairperson-arrested-over-posting-Museveni-in-coffin/688334-3485026-6lkhc9z/index.html

In 2017, David Mugema, a musician, and his producer Jonah Muwanguzi, were arrested and charged with offensive communication after they composed, recorded, produced and distributed a song which allegedly attacked and disturbed the peace of President Museveni.[37] Muwanguzi was also charged with promoting offensive communication by aiding Mugema in producing the song. In August 2019, Dr. Stella Nyanzi, an academic and human rights activist, was convicted of cyber harassment and sentenced to 18 months in jail.[38] Dr. Nyanzi was arrested in November 2018 and charged under sections 24(1) and (2)(a) of the Computer Misuse Act 2011[39] for using metaphorically worded poetry criticising President Museveni's reigna. Following an appeal against her conviction, Nyanzi was acquitted and released in February 2020.[40]

4.1.2 Disrupting Networks – From SMS Censorship to Social Media Blockage

Over the years, communication disruptions, including blocking of SMS and websites, filtering of content as well as shutting down of the internet, have emerged as one of the strategies used by the government to curtail freedom of expression and online communication. These shutdowns and attempts to block communication have occurred around elections times and during protests.

Early Years of Website and SMS Blockage

The year 2006 marked the start of a new range of communication disruptions related to elections in Uganda. In February 2006, Uganda's communications regulator instructed ISPs to block access to www.RadioKatwe.com, a website that published anti-government gossip. Authorities alleged that the website was publishing "malicious and false information against the ruling party NRM and its presidential candidate."[41]

In February 2011, the UCC directed telecom companies to block and regulate text messages that could instigate hatred, violence and unrest during the presidential election period. The regulator issued 18 words and names, which mobile phone SMS providers were instructed to flag if they were contained in any text message. Issued in the heat of the Arab Spring uprisings, these words included 'Tunisia', 'Egypt', 'Ben Ali', 'Mubarak', 'dictator', 'teargas', 'kafu' (it is dead), 'emundu' (gun), 'gasiya' (rubbish), 'army/ police/UPDF', 'people power', and 'gun/bullet'. Two UCC spokesmen confirmed the directive to local media, saying the aim was "to ensure free, fair and peaceful elections."[42] Two months later in April 2011, UCC ordered the shutdown of access to social media platforms such as Twitter and Facebook in April 2011 during the "Walk to Work" protests led by the runner-up in that year's presidential polls.[43]

37 *Musician arrested for disturbing Museveni's peace, https://mobile.nation.co.ke/news/africa/Musician-arrested-for-disturbing-Yoweri-Museveni-peace/3126394-4216504-1mpklhz/index.html*

38 *Al Jazeera, Ugandan academic Stella Nyanzi jailed for 'harassing' Museveni, August 3, 2019, https://www.aljazeera.com/news/2019/08/ugandan-academic-stella-nyanzi-jailed-harassing-museveni-190803141817222.html*

39 *Ibid*

40 *Harassing the president: Court orders immediate release of Stella Nyanzi, https://observer.ug/news/headlines/63597-harassing-the-president-court-orders-immediate-release-of-stella-nyanzi*

41 *CIPESA, Uganda's Assurances on Social Media Monitoring Ring Hollow, https://cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow/*

42 *Uganda bans SMS texting of key words during poll, http://www.reuters.com/article/2011/02/17/ozatp-uganda-election-telecoms-idAFJOE71G0M520110217*

43 *CIPESA (2016), State of Internet Freedom in Africa https://cipesa.org/?wpfb_dl=225*

Network Shutdowns Become Endemic

Around Africa, the year 2015 marked the start of widespread internet shutdowns and the practice remained prevalent well into 2019. In Uganda during the general election of February 18, 2016, the government through the UCC Executive Director ordered mobile operators to shut access to social media and mobile money services for national security reasons and to block people from "telling lies."[44] Furthermore, on May 13, 2016, during the presidential swearing-in ceremony, access to social media was shut down again. These measures forced a considerable number of internet users to bypass social network disruptions by use of Virtual Private Network (VPN).[45]

Disrupting networks through SMS censorship, social media blockage, internet throttling and internet total shutdown is a major threat to internet freedom as it effectively limits access to the internet, critical news and information especially during elections and other emergencies and limits one's ability to exercise their right to freedom of expression, association and assembly.

4.1.3 Surveillance Galore: The Build-Up of the State's Capacity

Given the existence of several provisions within the legal and policy frameworks, reports of surveillance and interception of communication in the country have been on the rise over the last couple of years. The government has continued to enhance its technical capacity to intercept and conduct surveillance.

Going High-Tech to Implement Surveillance

Buoyed by the enabling legal environment that provided for lawful interception, after the passage of the RICA, Anti-Terrorism Act and Anti-Pornography Act, the government then moved to enhance its mass surveillance capacity through use of spyware, intrusion malware, and intelligent network monitoring systems.[46]

A Privacy International report showed that by 2012, the government had installed FinFisher, a Wi-Fi and desktop intrusion malware, in the business centres of 21 hotels frequented by key opposition leaders, diplomats, and journalists.[47] Further, between April and July 2015, leaked emails of correspondence between Hacking Team, a malware manufacturer, and Uganda Police Force, revealed plans by the government to procure Hacking Team's premium Remote Control System (RCS), creatively named Galileo, sometimes Da Vinci.[48] The RCS system can copy files from a targeted computer hard disk, record skype calls, e-mails, instant messages, and passwords typed into a web browser, and access the device's webcam and microphone.[49]

In 2014, the local press reported that the government was planning to acquire a USD 54 million "phone tapping" machine that would have technical capacity to intercept email, phone calls, location data which would be reconciled in the national ID database.[50]

44 Museveni explains social media, mobile money shutdown, https://www.monitor.co.ug/News/National/Museveni-explains-social-media--mobile-money-shutdown/-/688334/3082990/-/rj5kk5z/-/index.html

45 Uganda Again Blocks Social Media to Stifle Anti-Museveni Protests, https://cipesa.org/2016/05/uganda-again-blocks-social-media-to-stifle-anti-museveni-protests/

46 Privacy International, State of Privacy Uganda, January, 2019, https://privacyinternational.org/state-privacy/1013/state-privacy-uganda#commssurveillance

47 https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

48 Daniel Mwesigwa, Leaked Emails: How Hacking Team and Uganda government want to spy on you, July 22, 2015, https://www.dignited.com/14494/leaked-emails-how-hacking-team-and-uganda-government-want-to-spy-on-you/

49 Bill Marczak, et. al., Mapping Hacking Team's "Untraceable" Spyware, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

50 Risdel Kasasira, Govt to buy Shs200b phone-tapping machine, December 13, 2014, https://www.monitor.co.ug/News/National/Govt-to-buy-Shs200b-phone-tapping-machine/-/688334/2554336/-/j26r4mz/-/index.html

In August 2016, Uganda's Minister of Ethics and Integrity, Fr. Simon Lokodo, announced that the government would procure a USD 88,000 "porn detection machine" to stamp out pornography from the country's infosphere.[51] While this claim attracted questions as to how exactly the "porn machine" would work, the minister's announcement was followed by the blocking of select pornography websites.[52] Since then, the government has employed a mix of techniques including technical interventions and the introduction of various regulations to control the internet. In July 2017, it was reported that the Chinese government had agreed to offer Uganda a comprehensive cybersecurity solution to reportedly monitor and tackle social media abuse.[53]

In January 2018, it was reported that UCC had set up a Centralised Equipment Identity Register system in a bid to identify, and stamp out fake and illegal mobile devices said to be hazardous to health and used to commit crime.[54] In July the same year, UCC installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification.[55] The system is hosted on communications infrastructure owned by mobile network operators, and the UCC can monitor multi-vendor data, network performance, and customer experience records, among others.[56] The president had long accused telcos of tax evasion and under-reporting revenues to the government.[57] In June 2019, it emerged that Uganda Telecom, the government-owned mobile operator, was the only one of five major licensed telcos that had not yet installed the INMS, thus posing a "national security threat".[58]

In 2018, the government commenced the installation of CCTV cameras in Kampala capital city and surrounding areas in an attempt to curb the spate of assassinations and urban crime that had gripped the country.[59] However, the high-profile killings and cases of homicide remain at large. In August 2019, The Wall Street Journal published an investigative piece detailing how Huawei had helped the Uganda Police Force to infiltrate encrypted communication channels used by a key opposition leader.[60] Notably, it also mentioned Uganda's plans to open a new six-story USD 30 million hub in November 2019, which would be linked to the over USD 126 million "Smart Cities" project implemented in Uganda by Huawei. The project entails the installation of CCTV surveillance cameras equipped with Huawei facial-recognition (AI) technology.

However, whereas Uganda enacted a data protection and privacy law in early 2019, the lack of regulations to operationalise the law and the inadequacy of ethical standards and requirements to manage sensitive data, threaten the rights to privacy and freedoms of expression and assembly. For example, the unexplained leakage of footage from police CCTV cameras in Kampala raises questions on standards and requirements to manage the retrieval, sharing and erasure of public CCTV footage.[61]

51 *Martin Kitubi, Pornography detection machine arrives September - Lokodo, August 2, 2016, https://www.newvision.co.ug/new_vision/news/1431545/pornography-detection-machine-arrives-august-lokodo#sthash.ti3VGka4.dpuf*

52 *Andrew Bagala, Pornography sites blocked, December 6, 2018, https://www.monitor.co.ug/News/National/Pornography-sites-blocked/688334-4883140-sj3hbo/index.html*

53 *Yasiin Mugerwa, China to help Uganda fight Internet abuse," July 26, 2017, https://www.monitor.co.ug/News/National/China-Uganda-Internet-Evelyn-Anite-Africa-Internet-Users/688334-4032626-u1l61r/index.html*

54 *Unwanted Witness, Uganda Communication Commission sets up mobile phone monitoring system, https://unwantedwitness.or.ug/uganda-communication-commission-sets-up-mobile-phone-monitoring-system*

55 *ITWeb Africa, Uganda's UCC, telcos clash over network monitoring technology, https://bt.ly/2NEMVON*

56 *Government installs system to track telecoms revenues, https://bt.ly/2OQDXU*

57 *All Africa, Uganda: Fight Over Shs.44Trillion Mobile Money, https://allafrica.com/stories/201802260042.html*

58 *Haggai Matsiko, Museveni buying Shs70bn gadget to monitor telecoms," May 9, 2016, https://www.independent.co.ug/museveni-buying-shs70bn-gadget-to-monitor-telecoms/*

59 *Vision Reporter, Museveni commissions CCTV cameras, October 9, 2018, https://www.newvision.co.ug/new_vision/news/1487292/museveni-commissions-cctv-cameras*

60 *Joe Parkinson, et al., "Huawei Technicians Helped African Governments Spy on Political Opponents, August 15, 2019,https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017*

61 *Daniel Mwesigwa, "Cameras, mobiles, radios – action!': old surveillance tools in new robes in Uganda. Uganda country report in Global Information Society Watch 2019, https://www.giswatch.org/node/6194*

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

Once the government was able to intercept communication, resolving the identity question then remained a matter of time. Measures have been introduced progressively to enable the government to precisely identify all telecommunication services users. During the 2010-2015 period, Uganda introduced massive personal data collection programmes. This was despite the absence of data protection laws. From SIM card registration, the government has since adopted digital identities, albeit with poor or no oversight.

Mandatory SIM Card Registration

The registration of SIM cards was made mandatory in Uganda in 2012 following a campaign by the UCC to fulfil its mandate under the Regulations of Interception of Communications Act (2010). The commission stated that the exercise was necessary to curb crime by enabling the tracking of criminals and identification of mobile phone SIM card owners. According to the government, criminals were using unregistered SIM cards and counterfeit phones to commit crimes such as theft and murder. The state also argued that the registration was important to stamp out counterfeit mobile devices, in other words, mobile phones that did not have legitimate International Mobile Equipment Identity (IMEI) numbers and thus posed security and environmental risks. In December 2013, the High Court declined to hear the case by Human Rights Network for Journalists-Uganda (HRNJ-Uganda) and Legal Brains Trust challenging the SIM card registration exercise. The Court argued that the SIM card exercise had ended on August 31, 2013 and that it would be futile to litigate retrospectively. Further, in a High court ruling on May 18, 2017, judge Steven Musota dismissed another case seeking to block the UCC from deactivating all unregistered SIM cards by May 19, 2017.

Post 2015, on April 12, 2017, the UCC issued a seven-day ultimatum for citizen subscribers to update their SIM card registration details using only valid national Identity (ID) cards to curb the recent wave of physical and cybercrime allegedly executed with the help of unregistered mobile phones. The Uganda Law Society termed this ultimatum as illegal citing, among other things, that the Registration of Persons' Act allows valid identification documents issued by government agencies such as national ID cards, work permits, passports, driving licence, student Identity cards and voter's cards to be used for registration.

On March 28, 2018, UCC issued a directive banning the sale of new SIM cards with new guidelines requiring telcos to use national ID card readers to electronically verify registration data against the national ID register maintained by NIRA. In April 2018, the Parliament resolved to extend the SIM card registration by not more than one year, however, Frank Tumwebaze, the Minister of ICT and National Guidance responded on Twitter that, "Government notes and will address issues of Parliament in regard to the SIM-card verification period, the deadline stands." UCC, however, lifted the ban after NIRA gave them 50 biometric machines to facilitate the capturing of user biodata.

The double collection of personal data could possibly imply that the data is used beyond what it was initially collected for, contrary to established international best practices.[62] Besides, there has not been sufficient evidence that indeed mandatory sim card registration reduces crime.[63] However, as some critics argued previously when SIM card registration started, the massive collection of personal data, without proper oversight, poses a threat to privacy and freedom of expression.[64] In fact, there have been recent cases of identity theft and cyber fraud committed through use of registered SIM cards. In 2018, SIM cards belonging to Members of Parliament (MP) were cloned and used in a SIM card duplication fraud, a sophisticated form of fraud that allows hackers to gain access and control a user's phone number. The Parliamentarians included Western Youth MP Mwine Mpaka and Eastern Youth MP Ishma Mafabi who reported how they were hacked in a similar manner where their numbers were used by hackers to solicit for funds from friends, colleagues, and family.

Adoption of Biometric Data Collection

The Electoral Commission of Uganda first introduced a biometric voter register in 2001 with the implementation of the Photographic Voter Registration and Identification Systems (PVRIS) project, becoming one of the first adopters of biometrics in Africa, although the system was first successfully used countrywide in the 2006 elections.[65] For the 2011 elections, the Biometric Voter Registration system was introduced by using equipment acquired under the National Security Information System (NSIS) project, which was being implemented by the Ministry of Internal Affairs. However, in 2013, the need to centralize citizen registration across MDAs – such as Directorate of Citizenship and Immigration Control, the National Information Technology Authority Uganda, the Uganda Registration Services Bureau, the Uganda Bureau of Statistics and supporting agencies, including the Uganda People's Defence Force, the Uganda Police Force and the Uganda Prisons Service – and the need to mitigate the duplication of resources, the government kicked off the biometric voter registration alongside the national identification registration process with these overarching objectives:

- identify and register Ugandan citizens and issue them unique national identification numbers and national ID cards;
- register citizens 16 years of age and older for the purpose of producing a clean voter register in time for use in the 2016 elections;
- register resident aliens and issue them alien ID cards.

For the 2016 elections, the Electoral Commission extracted data from the NIRA national ID database to compile the national voter register. Fraught with inconsistencies and errors, the electoral body was called out by a team of activists for flaunting the voter register with 20,000 ghost voters.[66] Further analysis in the voter register revealed that areas of stronger opposition in the previous elections could have been deliberately weakened through reduction of voter numbers in spite of the increasing demographics in those areas.[67] The unfettered access to the national ID database by different bodies, including security and law enforcement and private sector corporations such as telecom and technology service providers raises questions on the ability of arbitrary actors to abuse very sensitive personally identifiable information during electoral cycles.[68]

62 *Edrine Wanyama, "The Stampede for SIM Card Registration: A Major Question for Africa, April 18, 2018, https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/*

63 *Ibid.*

64 *Law requiring registration of SIM cards in Uganda a threat to privacy," September 24, 2012, https://ifex.org/law-requiring-registration-of-sim-cards-in-uganda-a-threat-to-privacy/*

65 *Available at https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf*

66 *Gaaki Kigambo, "Doubts still linger over accuracy, integrity of Uganda electoral body's list," February 13, 2016, available at https://www.theeastafrican.co.ke/news/Doubts-still-linger-over-integrity-of-Uganda-voter-list-/2558-3075122-view-printVersion-d9830nz/index.html*

67 *Available at https://medium.com/@valanchee/is-electoral-commission-deliberately-weakening-opposition-strongholds-757f64d27d33*

68 *Claire Lee, "Dispute in Uganda over Mobile Money Monitoring Continues," March 15, 2018, available at https://dfsobservatory.com/content/dispute-uganda-over-mobile-money-monitoring-continues*

4.1.5 Enter The Era of Social Media and Data Taxation

In the more recent past, the state has taken stern policy and regulatory positions to undermine internet freedoms. One of the notable and concerning phenomena is the use of taxation to undermine citizens' use of the internet. In some instances, such measures have been designed partly to limit citizens' access to digital technologies and to hold the government accountable.

In May 2018, the government passed an amendment to the Excise Duty Act, introducing a mandatory tax of UGX 200 (USD 0.05) per user per day for access to OTT services such as WhatsApp, Facebook and Twitter.[69] In the same amendment, a 1% levy was imposed on all mobile money cash withdrawal transactions, an issue that caused public outcry and prompted parliament to reduce the levy to 0.5%. In a letter to the Finance Minister in March 2018, President Museveni wrote that the taxes were necessary as the country needed resources to cope with the consequences of "olugambo on social media (opinions, prejudices, insults, friendly chats) and advertisements by Google".[70]

Earlier in April 2018, the Ugandan communications regulator had directed online data communication service providers, including online publishers, online news platforms and online radio and television operators, to apply and obtain authorisation from the commission within a period of one month or risk having their websites and/or streams being blocked by Internet Service Providers (ISPs).[71] The regulator later published a list of the licenced providers, who were each required to pay USD 20 per annum. Later in 2019, the Ugandan regulator announced that "online publishers and individual influencers with heavily followed social media and other online accounts that carried ads alongside other content on platforms including Twitter, Facebook, Instagram and YouTube had to register with UCC and pay a USD 20 levy per annum.[72] Comments from sections of the public and media highlight dissatisfaction with UCC's methods of work citing regulatory decisions of political nature meant to derail social media savvy youth from publicly calling out aging political leaders. A media practitioner added that mandatory registration of bloggers and influencers threatens press freedom.[73]

Consequently, digital taxation has had a major impact on the use of internet-based platforms such as social media: For instance, Uganda's usage of the internet usage has dropped, implying reduced enjoyment of digital rights; while internet penetration has declined, as has internet service delivery.[74]

69 CIPESA, Uganda: New social media tax will push basic connectivity further out of reach for millions,https://cipesa.org/2018/06/uganda-new-social-media-tax-will-push-basic-connectivity-further-out-of-reach-for-millions/

70 Elias Biryabarema, "Uganda to register, monitor social media influencers," August 8, 2019, available at https://www.reuters.com/article/us-uganda-communications/uganda-to-register-monitor-social-media-influencers-idUSKCN1UY265

71 See The Registration Of Online Data Communication And Broadcast Service Providers notice at http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf

72 Apollo Mubiru and Lucy Kiiza, UCC registers online publishers and influencers, https://www.newvision.co.ug/new_vision/news/1504833/ucc-registers-online-publishers-influencers

73 Halima Athumani, "Ugandan Online Publishers Criticize Registration as Political Control," August 4, 2019, available at https://www.voanews.com/africa/ugandan-online-publishers-criticize-registration-political-control

74 Juliet Nanfuka, "Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%," January 31, 2019, available at https://cipesa.org/2019/01/%ef%bb%bfsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/; Juliet Nanfuka, "How Social Media Taxes Can Burden News Outlets: The Case of Uganda," March 16, 2019, available at https://cipesa.org/2019/05/how-social-media-taxes-can-burden-news-outlets-the-case-of-uganda/

4.2 Key Positive Developments

Despite the negative trends witnessed, there were notable developments that were indeed and that supported the enjoyment of internet freedom. The three major developments included the robust advocacy and push-back by non-state actors, the adoption of progressive legislation and lastly, the repeal of repressive legislation.

4.2.1 Robust Advocacy and Push-back by Non-State Actors

The changing legal landscape has played an important role in the promotion of internet freedom, with various civil society organisations championing internet freedom in Uganda. Through research and documentation, the organisations have been able to draw attention to breaches to internet freedom in a range of cases. They have also conducted advocacy and awareness-raising, and instituted strategic digital rights litigation.

4.2.2 Repeal of Repressive Legislation

In 2004, the Constitutional Court declared unconstitutional section 50 of the Penal Code which made the publication of false news a criminal offence. This was a result of the petition filed by Charles Onyango Obbo and Andrew Mwenda against. Attorney General. In his lead judgement, Justice Joseph Mulenga held that, "extending protection of the freedom of expression to false statements does not necessarily defeat the objective of upholding the truth, because while truth and falsity are mutually exclusive, the purposes for protecting both are not".[75]

In another case of Charles Onyango Obbo and Andrew Mwenda vs. Attorney General (2010), the Constitutional Court declared sections 39 and 40 of the Penal Code, which related to edition, null and void. In the case, the state alleged that Mwenda's remarks on a popular radio talk show, including the allegation that the government was partly responsible for the death of South Sudan John Garang, were intended to bring hate and contempt against the president, government, and constitution. The then Deputy Chief Justice, Leticia Mukasa Kikonyogo, delivered the unanimous ruling that, "[sedition] is so wide and it catches everybody to the extent that it incriminates a person in the enjoyment of one's right of expression of thought. Our people express their thoughts differently depending on the environment of their birth, upbringing and education."[76]

4.2.2 Adoption of Progressive Legislation

The enactment of the Access to Information Law in 2005, and the Data Protection and Privacy Act in Uganda in February 2019d were positive steps, given that the passing of the Data protection law coincided with an aggressive push for CCTV camera installation and other activities that engender massive data sweeps.[77] On the other hand, the access to information law boosted Uganda's openness to scrutiny and accountability with the government taking some steps to promote the right of access to information through a number of initiatives, including the development of the Government Communication Strategy to "establish an effective, well-coordinated and proactive communication system across Government and with the public that will meet the nation's information need".[78]

75 Joseph Mulenga JSC in Charles Onyango Obbo and Andrew Mwenda vs. Attorney General S.C.C.A No. 2 of 2002 [2004]
76 Charles Onyango Obbo and Andrew Mwenda vs. Attorney General, C.P. no. 12 of 2005 [2010]
77 Available at https://ulii.org/ug/legislation/act/2019/1
78 CIPESA (2017), The State of Access to Information in Uganda, https://cipesa.org/?wpfb_dl=241

5 Conclusion and Recommendations

5.1 Conclusion

It is evident that the government has continued to assert control over the internet in the last 20 years and broadened the range of measures to control the use of the internet and other digital communications. Indeed, the internet's centrality in everyday life has grown, and it has become increasingly perceived as a threat to authoritarian rule as it provides swift and affordable means for organisation and mobilisation. In a bid to control the internet's reach and influence in Uganda, the government has used a range of technical and legislative interventions.

On the legislative front, the government has passed laws and policies with far-reaching impact and used them to legitimise internet controls and to silence voices critics and dissenters. Technical measures have included network disruptions, SMS blockages, interception of communication, and other sophisticated surveillance measures.

However, the state of internet freedoms could be improved if strategies such as advocacy, partnership building and public interest litigation are drawn with the aim of promoting a favourable environment for their protection, enjoyment and enforcement of digital rights. In this, the role of civil society cannot be over-emphasised.

5.2 Recommendations

The following emerge as action points for the different stakeholders for the realisation of digital rights and freedoms.

Government

- Repeal all repressive laws and policies such as the social media tax so as to promote inclusive internet and information access.
- Fast track the implementation of the Data Protection and Privacy Act, 2019 to ensure compliance with the key data protection principles and data standards for data collection, storage and processing.
- The Uganda Human Rights Commission should establish a mechanism to monitor and review the status of the enjoyment of digital rights and to advise all stakeholders on best practices.

Companies

- Adopt and implement the UN Business and Human Rights principles and safeguard the rights of customers by default.
- Establish partnerships and cooperate with the government and other stakeholders on initiatives such as policy and legal reforms that promote internet freedom in the country.
- Be transparent and independently publish reports on issues around internet freedom breaches such as state information requests and surveillance programmes.

Media

- Report on and conduct investigative stories on contemporary issues affecting internet freedom in the country such as network disruptions, surveillance, arrests and censorship.
- Educate the general public, especially the youth through stories, debates and conversations on internet freedom so as to empower them with knowledge to enable them influence and shape the internet landscape.
- Interpret and disseminate research findings from academia, the technical community, and other relevant bodies so as to enhance public knowledge and eminent actions on internet freedoms.

.

Academia

- Collaborate with different stakeholders in government, private sector, media and civil society to conduct evidence-based research on affronts to internet freedom.
- Build more and stronger collaborations with digital rights experts such as lawyers, activists, civil society actors, bloggers and other practitioners in order to share knowledge, learnings and best practices on internet freedoms in Uganda and Africa.
- Provide safe spaces for intellectual deliberations on issues of internet freedom. This could for example be through organising seminars and conferences.

Technical Community

- Advise the government, telcos and internet service providers and other relevant bodies on important steps to take to promote internet freedom.

Civil Society

- Build more communities of practice to address the challenges and opportunities for the promotion of internet freedom.
- Support joint efforts and build partnerships to support digital rights promotion, including those that conduct advocacy and litigation.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org