State of Internet Freedom in Uganda 2016

Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights

December 2016

CIPESA

State of Internet Freedom in Uganda | 2016

Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of the OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes Internet freedom in Africa.

The report presents the findings of a study on what the government in Uganda is doing to inhibit citizens' access to ICT, for example content blocks, censorship, filtering, infrastructure control, law-making, court cases; using ICT activity and data to monitor citizens; and how government bodies and functionaries are using propaganda, impersonation, threats, cloning, and other tactics to shape online content in their favour. Other country reports for Burundi, Democratic Republic of Congo, Ethiopia, Kenya, Rwanda, Somalia, Tanzania, Zambia and Zimbabwe as well as a regional State of Internet Freedom in Africa 2016 report, are also available.

CIPESA recognises Peter Magelah as the main content contributor to this report.

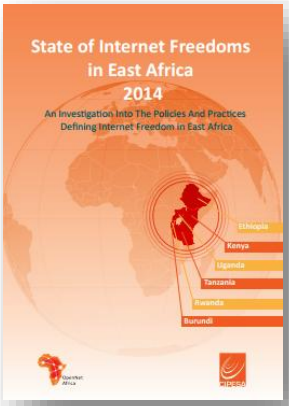
The research was conducted with support from Facebook and Google.

Editors
Ashnah Kalemera, Lillian Nalwoga, Juliet Nanfuka, Wairagala Wakabi, PhD

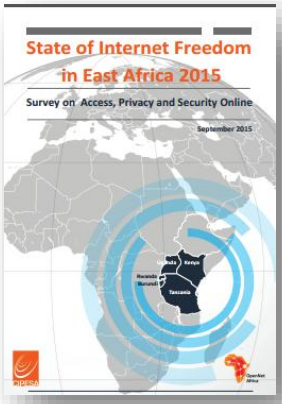
Design
Ish Designs
muwonge_issa@yahoo.com

State of Internet Freedom in Uganda 2016: Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights
Published by CIPESA | www.cipesa.org
December 2016

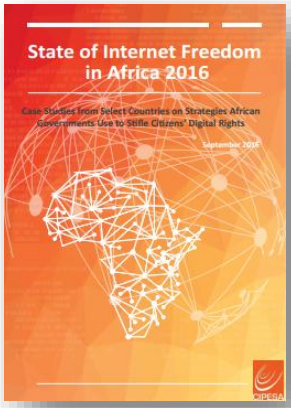
Reports in the State of Internet Freedom in Africa Series



[State of Internet Freedom in East Africa 2014]



[State of Internet Freedom in East Africa 2015]



[State of Internet Freedom in Africa 2016]

Country reports are also available on the CIPESA [Resources] page

Follow **#InternetFreedomAfrica** to see what others are saying and to share your thoughts.

Contents

1. Introduction

The Internet is increasingly becoming a significant tool for social, economic, and human rights development in Uganda and Africa at large. Average citizens, human rights activists, civil society organisations, media houses, and more recently, politicians and government institutions, have taken to various forms of social media – especially Facebook, WhatsApp and Twitter - for expression, association, and information sharing.

With this growing trend, many Ugandans are weighing in on social, economic, and political events, and starting campaigns and discussions that not only inform, but demand action and change. But for the internet to truly make an impact in any society's socio-political arena, it has to be accessible, affordable, and most of all, users must be able to enjoy the freedom to express their views and opinions. While accessibility and affordability of the internet in Uganda are positively blooming, the realisation of rights on the platform is still an area faced with challenges and restrictions, one being a notable increase of abuse, by both state and non-state actors, who violate users' privacy and freedom of expression.

Uganda is governed under a multi-party political system, with 29 registered political parties.[1] The most recent presidential elections held in February 2016 saw President Yoweri Museveni of the National Resistance Movement (NRM) re-elected for a fifth term in office. During the election campaigns, reports of voter intimidation and harassment of opposition leaders were rampant, especially from the camps of the Forum for Democratic Change (FDC) led by Kizza Besigye and that of former Prime Minister Amama Mbabazi, who were both contesting against President Museveni.

As Uganda went to elections in early 2016, there was a focus on using social media to campaign and garner votes. Nearly all the presidential candidates used social media to reach out to the youth and other voters who use social media. Campaigning on social media also saw an increase in sharing of false information, violation of rights such as sharing of personal and private information, as well as attempts to control use of social media.

Uganda, like many African governments, has put in place laws like the Computer Misuse Act 2011, Electronics Transactions Act 2011 and Electronic Signatures Act 2011, among others, to ostensibly boost access to online information, combat cybercrime and protect internet users. However, many of these laws are seen by both citizens and activists as a way to stifle online rights, violate individuals' privacy, and hinder their freedom of expression. When feeling threatened by certain information that has been exposed online, the government of Uganda has been known to limit citizens' access to the internet, in the name of national security. Many internet users, particularly those on social media during the general elections held in early 2016, had to resort to using proxies and secure Virtual Private Networks (VPNs) to access information after the national communication regulator, the Uganda Communications Commission (UCC), ordered service providers to block access to popular social media platforms.

Meanwhile, the mandatory SIM registration for all phone users and the national identity card project under the National Identification and Registration Authority are also viewed with suspicion by certain sections of society, pointing to the fact that information collected from these exercises may be used by the government to spy on citizens.

[1] Registered Political Parties, http://www.elections.co.ug/new-vision/election/1000171/registered-political-parties/page/1

The research results presented in this report focus on recent legal and policy developments, as well as on abuses and violations of internet freedom spanning 12 months to November 2016. However, in order to establish trends on strategies of information controls used by the government of Uganda, the study takes an interest in practices over the last five years.

2. Research Methodology

The research presented in this report was conducted through a mixed methods approach. Researchers based in Uganda interviewed key informants who were purposively selected. The informants were chosen on the basis of their knowledge about issues related to or affecting internet freedom in the country. They included activists and human rights defenders that are advancing free expression and association in these countries, as well as some of those who had been victims of abuses and violations. Others were internet and telecom service providers, regulators, law enforcement officials, and journalists. In total, 11 key informants were interviewed for this report.

Policy analysis was conducted to generate an understanding of the existing and proposed laws that affect digital rights. The analysis took an interest both in policies and laws that have been used to curtail internet freedom and those that could potentially be employed in curtailing freedom of expression and access to digital technologies. Analysis was done of relevant Bills currently under consideration by parliament. Moreover, document review was done, including of open access sources such as media articles and secondary research reports, as well as analysis of records such as court orders and regulatory decisions, some of which are not readily available in the public domain.

3. Country Context

3.1 Access

According to the latest figures from the Uganda Communications Commission, Uganda has an estimated 15.5 million Internet users, with a 46% penetration rate. Over 22.3 million Ugandans are telephone subscribers (both fixed and mobile), and the national telephone penetration stands at 61.[2] This rapid growth can be attributed to the increased investments in the ICT sector by both the government and the private sector, the availability of smart cheap phones on the Ugandan market, and a steady reduction in voice and data costs.[3]

Uganda has five major mobile network operators – MTN, Airtel, Africell, Vodafone, and Uganda Telecom. Smaller service providers include Smart Telecom, Smile Telecom, and K2 Telecom. With such a competitive market, and the presence of numerous low-price internet service providers (ISPs), internet and voice prices continue to go down. Currently, the average cost for a daily 10MB mobile Internet bundle

[2] UCC, Post, Broadcasting and Telecommunications Market and Industry Report, July-September 2016; http://ucc.co.ug/files/downloads/Market_&_Industry_Report_for_Q3_July-September_2016.pdf

[3] An Overview of How ICT Policies Infringe on Online Privacy and Data Protection, CIPESA ICT Policy Briefing Series No. 06/15 December 2015, http://www.cipesa.org/?wpfb_dl=201

is as low is 300 Uganda Shillings (UGX) (about USD 10 cents), while a monthly 1GB bundle costs between UGX 25,000 – 40,000 (USD 7-11), depending on the provider.[4] Other product promotions such as free or subsidised access to Whatsapp, Twitter and Facebook from some providers have also contributed to the high level of connectivity among Ugandans.

In addition, the government has also established institutions such as the Ministry of ICT, and National Information Technology Authority of Uganda (NITA-U) to provide strategic and technical leadership and guidance to the ICT sector. Through NITA-U, the National Data Transmission Backbone Infrastructure and e-Government Infrastructure Project (NBI/EGI) set out to connect all major towns in Uganda onto an optic fibre cable based network, as well as to connect all government Ministries, Department and Agencies (MDAs) onto one e-Government network. The country's national fibre backbone is connected to the East African Submarine cable System (EASSy), an international submarine fibre-optic cable system that runs along the east and southern coasts of Africa. Telecommunications providers are also hooked to The East African Marine System (TEAMS) and SEACOM marine fibres through Kenya. The NBI/EGI project has to-date installed 1,590km of fibre optic cable across the country and connected 135 MDAs to the backbone. Seven public universities have also been connected to the national backbone, ICT has been integrated into the secondary school curriculum, and over 1,000 ICT labs have been established in different schools.[5]

3.2 Laws and Policies Affecting Internet Freedom

Uganda has over the years enacted a number of laws aimed at regulating the use of the internet. Whereas the general purpose of the laws is to facilitate use of Internet and protect users from possible negative outcomes such as cybercrime, a number of laws have restrictions that limit the enjoyment of Internet freedom. In this section, we review laws that tend to hinder freedom of expression, including Internet freedom.

The **Uganda Communications Act, 2013** seeks to consolidate and harmonise the regulation of communications and electronic media in Uganda.[6] The Act sets up the Uganda Communications Commission (UCC) as a regulatory body for all electronic communication systems in Uganda. The law gives UCC several powers, which range from regulating the sector, setting up policy, monitoring of the sector, licensing and enforcing laws relating to the communications sector, fining and punishing those who violate the law. Although the Act provides for establishment of a Communications Tribunal whose role is to be an arbitrator on issues relating to the communications sector, to-date this has not been done.[7] The lack of a tribunal has also resulted in a situation where the UCC can be a complainant and a judge in cases and this presents a potential for miscarriage of justice.

In the last year, UCC used its powers under this Act to issue directives for the blocking of social media and mobile money access during national elections and at the swearing in ceremony of the president. The regulator claimed the blockage was necessary for the security of the country. The blockage was condemned by various human rights organisations as a violation of the right to freedom to expression and other Internet freedoms.

[4] See http://kompare.ug/internet/mobile-internet/
[5] The National Backbone Infrastructure Project (NBI/EGI)
- http://www.nita.go.ug/projects/national-backbone-infrastructure-project-nbiegi
[6] Act 1 of Uganda Communications Act, 2013
[7] See Part X of Uganda Communications Act, 2013

On February 26, 2016, the Minister of Information and Communications Technology gazetted the **Communications (Amendment) Bill, 2016** that seeks to amend section 93(1) of the Communications Act, 2013 to enable the minister to make statutory instruments without seeking parliamentary approval. The current law requires the minister to lay regulations before parliament for approval, hence the amendment would be an attempt at ousting parliamentary oversight powers.[8]

The Amendment not only removes the requirement for parliamentary approval for regulations made by the minister under the Act, but also the requirement to inform parliament of the new legislation made through laying the regulation before parliament. This move violates Article 79 of the Constitution of Uganda, which gives parliament the overall powers to make laws and any other institution that makes laws such as subsidiary legislation can only do it with the consent of parliament.[9] It is therefore important that the institution that delegates the powers to make laws remains with the powers to approve the laws, to be informed of the laws made and to withdraw or suspend the law made under delegation.

The Computer Misuse Act, 2011 seeks to provide for safety and security of electronic transactions and information systems and to prevent unlawful access, abuse or misuse of information systems among other things.[10] The Act has a broad definition of a computer, which covers all types of electronic or electromagnetic systems capable of storing or transmitting data. The broad definition of a computer means that any person using an electronic or electromagnetic system has a duty to act within the confines of the Act, failure of which is one of the several offences under the Act. The broad nature of this Act was tested in Nyakahuma vs. Uganda[11] where, in a high court reference to determine whether posting materials on internet amounted to publication within the meaning of the Penal Code Act,[12] the judge ruled that the broad nature of the Computer Misuse Act captured all forms of posts made in cyberspace irrespective of the tool used to post.

Section 25 of the Act calls for the punishment of "offensive communication" where "any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding Uganda Shillings 480,000 (about USD 140) or imprisonment not exceeding one year or both". This provision is broad and has been abused by authorities to limit freedom of speech by prosecuting individuals deemed to have violated this section. As such, this section has been challenged in the constitutional court for being overly broad and unnecessary and likely to result in abuse of freedom of expression.[13]

On a positive note, the Act prohibits unauthorised access to a computer or computer systems and tries to regulate any form of hacking that may occur whether online or a standalone system. It also gives court

[8] HRNJ (2016) Analysis of the Uganda Communications (Amendment) Bill 2016, https://hrnjuganda.org/?page_id=2639

[9] Article 79 of the Constitution of Uganda, 1995

[10] Act No. 2 of the Computer Misuse Act, 2011

[11] High Court criminal reference No 1/2013 available at http://www.ulii.org/ug/judgment/high-court-criminal-division/2013/30-0

[12] Cap 120, laws of Uganda

[13] See Andrew Karamagi and Shaka Robert Vs. AG. Constitutional Court Petition No. 5 of 2016. The background to this case is Shaka Robert was charged with offensive communication under Section 25 of the Computer Misuse Act after government officials believed him to be Tom Voltaire Okwalinga who pseudonymously posts information critical of government on Facebook. Shaka challenged the law under which he was charged and at the time of writing this report court decision was still pending.

powers to make a preservation order where data that is subject to investigation or a court case is at risk of being damaged or lost.

Other laws relating to cybercrime offenses include the Electronic transactions Act, 2011 and Electronic Signature Act, 2011, which regulate e-commerce but remain mostly unimplemented.

Meanwhile, the **Anti-Pornography Act, 2014** prohibits the publication and circulation of pornographic content. Section 2 of the Act defines pornography as "any representation through publication, exhibition, and cinematography, indecent show, information technology or by whatever means of a person engaged in real or stimulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual excitement." This definition of pornography has been criticised for being too broad and open to misinterpretation.[14] Section 13 makes it an offence to publish, broadcast, traffic in, procure, import or export pornography. The law is mostly unfavourable to women as section 13 is likely to discourage victims of revenge pornography from reporting cases to authorities in fear of retribution as the victim and perpetrator are equally liable. Moreover, section 17 requires Internet Service Providers (ISPs) not to allow their protocols and systems to be used for publishing pornography. It places an obligation on ISPs to monitor and carry out surveillance on their customers for them to be able to identify and remove content considered pornographic.

Generally speaking the broad nature of an offence under the Anti-Pornography Act 2014 Act is bound to affect various Internet users who may in one way or the other be in possession of content considered pornographic. For example, whereas in some countries courts have ruled that using the "like" button on social media such as Facebook does not give rise to action in defamation,[15] it is not clear if "liking" a page with pornographic content can be adjudged as publishing pornographic content hence giving rise to criminal liability. It is also not clear how the law will treat cases where a person is found in possession of content considered pornographic which they accessed through social media such as Whatsapp, where he or she had no control on the process of distribution or download of the said content.

The Anti-Pornography Act, 2014 also calls for the establishment of an anti-pornography committee and in July 2016, a committee of eight members was set up.[16] In June and August 2016, claims of government purchasing anti-pornography detection software surfaced.[17] However, the ethics minister later denied the statements saying the government did not have enough funds to procure the software. Whereas restricting pornography, especially child pornography, is warranted, such restrictions should fall within internationally accepted standards. Blanket surveillance to snoop out pornography has bigger consequences such as limiting the right to privacy.

The right to privacy is further limited by the **Anti-Terrorism Act, 2002**, which provides for interception of communications.[18] The law does not define what an electronic system is; however, going by the definition

[14] See Lwawoko Jordan (2015) Gender and anti-pornography Act Uganda, http://www.academia.edu/7409096/gender_and_the_anti_pornography_act_uganda also see Unwanted Witness, Analyzed cyber laws of Uganda, 2016, https://unwantedwitness.or.ug/?wpfb_dl=47

[15] Crookes v. Newton [2011] 3 SCR 269, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7963/index.do accessed on October 15th 2016 also see Cairns v Modi [2012] EWHC 756 (QB)

[16] Pornography control committee named, http://www.newvision.co.ug/new_vision/news/1422110/anti-pornographic-committee-named

[17] Pornography detection machine arrives September – Lokodo, http://www.newvision.co.ug/new_vision/news/1431545/pornography-detection-machine-arrives-august-lokodo

[18] Section 7of the Anti-Terrorism Act 2002

provided by the Computer Misuse Act, any system capable of transforming electronic or electromagnetic data can be considered an electronic system. This means acts associated with online demonstration or expression of discontent such as hacking and bringing down government websites or interfering with their functionality can amount to terrorism in Uganda.

In 2015, amendments were made to the Terrorism Act to align the law to international requirements by providing for aspects of terror financing and money laundering. The coming into force of the amendment means police now has powers to conduct surveillance on online transactions with the aim of establishing if they are funding terror activities in Uganda.

The **Regulation of Interception of Communications Act, 2010** provides for lawful interception and monitoring of communications in the course of their transmission through a telecommunication, postal or any other related service or system. Section 3 provides for the establishment of a monitoring centre under the oversight of a minister. The Act makes it a crime to unlawfully intercept communication of a person and lawful interception is only permitted by authorised officials upon issue of a warrant by a judge.[19] The act also calls for service providers to technically assist government to intercept communications by installing hardware and software to enable interception of communications at all time or when required. Service providers are also required to provide services that render real time and full time monitoring facilities for the interception of communication where failure to do so is punishable with a fine of UGX 2,040,000 (about USD 583) or imprisonment for a period not exceeding five years, or both; and a possible cancelation of their license.

In 2014, Uganda embarked on drafting a Data Protection and Privacy law which followed wide public consultations. The bill seeks to protect the privacy of the individual and of personal data by regulating the collection and processing of personal data to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters.[20] In April 2016, the Draft Data Protection and Privacy Bill, 2016 received a first reading in Parliament but the bill is yet to be re-tabled in the current parliament.[21]

4. Results

4.1 Internet shutdowns

On Election Day in February 2016, social media platforms – Facebook, Twitter and WhatsApp - were shut down, as well as the popular mobile money services. The regulator, UCC, told local media houses that they had been directed to shut down the platforms over national security concerns. Ugandans had to resort to using VPNs to share information about the elections.[22] Another shut down was ordered again in May 2016, on the presidential inauguration day, and this trend has had some analysts believing that this

[19] ibid

[20] NITA-U (2016) Data Protection and Privacy Bill, 2016, http://www.nita.go.ug/publication/draft-data-protection-and-privacy-bill

[21] Parliament Watch,, http://parliamentwatch.ug/bills/data-protection-and-privacy-bill-2016/#.WG5Z33eZPdR

[22] Ugandans Turn to Proxies, VPN in Face of Social Media Shutdown,*http://www.opennetafrica.org/ugandans-turn-to-proxies-vpn-in-face-of-social-media-shutdown/*

practice will become a norm on the Ugandan political landscape.[23] [24] Some service providers such as MTN and Airtel informed their customers of the blockage while others did not. The regulator argued that the blockage was due to candidates' continued use of social media for campaigning and that there was information that people were using social media to incite violence.[25]

Nonetheless, the decision to block social media access received condemnation from both local and international actors since it violated freedom of expression. Further, the popular mobile money financial transfer system was also affected by the shutdown, leaving many citizens stranded while vendors faced losses due to the lack of transactions. The World Bank estimates that about 35% of Ugandans use Mobile Money services, making it the single most widely used system of money transfer and payments in the country.[26] The shutdown of mobile money platforms in Uganda did not only block access to this service but also affected access to a number of services that are paid for through this platform. These range from internet services, television subscription, utilities such as electricity and water to goods and services. Whereas there is no data as to the exact financial effect of such shut down, we can conclude that it affected the enjoyment of various rights in the country. Human rights watchdog Legal Brains Trust filed a suit against the social media blockage, which it said was detrimental not only to public welfare but also public confidence in the telecommunications and financial sectors. While urging court to order a lift to the blockage of the "unjustifiable and unlawful" blockage, the watchdog also wanted court to pronounce that the central bank, the Bank of Uganda, had "failed in its statutory duty to assert and protect its independence by swiftly issuing corrective directives to restore public access to mobile money services."[27]

Whereas Emilian Kayima, a spokesperson of the Uganda Police observed that there was a threat to security and the state had to block social media for safety and security of all Ugandans,[28] there was no government attempt before, during or after the blockage to show Ugandans that there was actual or potential threat of breach to security due to use of social media. This has left several observers suggesting that there were no security risks but rather a baseless censure to freedom of expression.

When questioned about the legal basis for the blockage, the Director Corporate Affairs at UCC observed that the Communications Act gives UCC broad powers and functions under Sections 5 and 6 and the regulator used the powers under this law to block social media and mobile money services.[29] Nonetheless it is noteworthy that the communications commissions received the orders to effect the blockage from the chief of police. In an affidavit filed on curt, the Executive Director of UCC stated, "In the early afternoon of 17th February 2016, I received a telephone call from the IGP [Inspector General of Police] who informed

[23] Social media shutdown in Uganda will become a norm, *http://acme-ug.org/2016/05/19/social-media-shutdown-in-uganda-will-become-a-norm-analysts/*

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

[25] Parliamentary elections in embarrassing mess, http://www.observer.ug/news-headlines/42678-presidential-parliamentary-elections-in-embarrassing-mess

[26] World Bank (2015) Global Inclusion Data available at http://datatopics.worldbank.org/financialinclusion/country/uganda

[27] Andante Okanya, Court petitioned over mobile money, social media blockade, http://www.newvision.co.ug/new_vision/news/1417691/court-petitioned-mobile-money-social-media-blockade

[28] Interview with Uganda Police spokesperson Emilian Kayima, September 2016

[29] Interview with UCC Corporate Affairs Director Fred Otunnu, September 2016

me that there was an imminent grave security concern by some individuals who wanted to use social media platforms and mobile money facilities to seriously destabilize security of the country."[30]

The two 2016 incidents were not the first instance that UCC ordered such a blockage. On April 14, 2011, it instructed ISPs to temporarily block access to Facebook and Twitter for 24 hours "to eliminate the connection and sharing of information that incites the public." The order came in the heat of opposition led 'walk to work' protests in various towns over rising fuel and food prices. The regulator's letter stated that the order had been prompted by a request from the security agencies that there was need to minimise the use of the media that may escalate violence. At the time, UCC Executive Director Godfrey Mutabazi told Reporters Without Borders that he would again order that access to Facebook and Twitter be cut off if it was in the interest of public safety.[31]

4.2 Using and Abusing Courts of Law to Stifle Internet Freedom

Uganda has over the last six years used laws to curtail Internet freedoms under the guise of protecting national security and cultural or moral values. Laws such as the Anti-Pornography Act, Anti-Terrorism Act and aspects of the Computer Misuse Act have justification for internet surveillance in Uganda. The laws limit freedom of expression, including in instances where such expression is considered immoral. For example, the Anti-Pornography Act prohibits any form of publication, culture or art that depict sex. The Computer Misuse Act on the other hand has vague provisions on what can amount to cyber stalking, among others. The Anti-Terrorism Act, Interception of Communications Act and Anti-Pornography Act give powers to the state and in instances to private entities to carry out surveillance to counter terrorism, monitor security or monitor publication of pornographic content or content deemed immoral.

These laws have been used to arrest and prosecute some social media users. In 2015, Robert Shaka was charged with offensive communication under Section 25 of the Computer Misuse Act after he was believed to be the identity behind TVO. Although Shaka was released on bail, the case was still pending a court decision at the time of writing this report.[32] In January 2016, former intelligence officer now political analyst Charles Rwomushana[33] was arrested and detained by police after he posted on Facebook a picture purporting to be the dead body of a bodyguard to an opposition presidential candidate who had gone missing.[34] In another incident, police in February 2016, arrested two youth for allegedly inciting violence and posting a picture of a dead president.[35] At the time of writing, it was unclear whether the case had gone to trial. Arrests of social media users have prompted many citizens and activists to practice self-censorship and others to use pseudonyms on social media. But as the case in section 4.2.1 below shows, anonymity rights in Uganda are under test and the results could have ramifications for internet freedom on the country.

[30] Kayihura Ordered Social Media Shutdown - UCC, http://allafrica.com/stories/201603180193.html
[31] State of Internet Freedom in Uganda 2014, http://cipesa.org/?wpfb_dl=181
[32] State of Internet Freedom in Uganda 2015, http://cipesa.org/?wpfb_dl=209
[33] Charles Rwomushana arrested over Aine pictures, http://www.ntv.co.ug/news/crime/09/jan/2016/charles-rwomushana-arrested-over-aine-pictures-10675#sthash.QtAu1aDn.dpbs
[34] Two months after the elections, the former bodyguard to opposition candidate Amama Mbabazi resurfaced, claiming he had fled to Kenya due to fear for his life.
[35] Two arrested over 'dead' Museveni picture, http://www.monitor.co.ug/News/National/Two-arrested-over--dead--Museveni-picture/688334-3106714-11plidxz/index.html

4.2.1 The Test of Anonymous Rights in Uganda, Muwema vs. TVO

The use of anonymous names and the rights of anonymous people in Uganda has not been tested in local court. However a user, who goes by the name Tom Voltaire Okwalinga (TVO) on Facebook, has over time developed a reputation for publishing information critical of the government, including what is labelled government secrets. Some of the information shared has come to pass as true, while some of it is false and some can be categorised as propaganda aimed at achieving particular aims.

In May 2016, Fred Muwema a prominent lawyer, requested Facebook to reveal the true identity and page of TVO, so he could sue him for defamation. Muwema's request followed TVO's publication on his Facebook page that Muwema had stage managed an attack on his law firm and had been bribed not to represent former presidential candidate Amama Mbabazi, who was petitioning the election results. Following Facebook's refusal to reveal the name and to delete TVOs page, Muwema sued Facebook in Ireland for court to grant the same orders.[36] In August 2016 ordered to reveal the identity of TVO to Muwema who could then institute proceedings against him back in Uganda. He however rejected the lawyer's request for Facebook to bring down the defamatory content posted against him, arguing that it had been widely circulated.[37] But Facebook denied it had a duty to remove the material particularly in circumstances where much of it is available across the internet by simply Googling "Muwema" and "bribe".[38] Moreover, it appalled against the order to reveal the identity of TVO, claiming that he would face reprisals including from state authorities. Facebook argued that government of Uganda had previously sought the identity of TVO and that revealing it would result into increased violation to TVO and other human rights defenders using their platform in Uganda.[39]

The case of Muwema Vs. Facebook Ireland Ltd stands to test online safety and user rights in Uganda. Facebook's key contention in the case is that revealing the identity of TVO will have far reaching human rights consequences including on freedom of expression, the fear of arrest and possible attacks on TVO by government of Uganda. In its additional affidavit filed on August 19, 2016, Facebook revealed that UCC boss, Godfrey Mutabazi, and the Uganda Police had previously written to Facebook requiring it to delete the page TVO or to put down posts made by TVO and Facebook rejected the requests.[40]

The present case surrounding TVO presents a landmark test on protection of freedom of speech online and whether a service provider can reveal the identity of a person where issues of human rights are engaged. It should be noted that in other jurisdictions such as the US and Canada, courts have held that a person has a right to remain anonymous online provided that has not been used to violate rights of others and that an anonymous person has the same rights and protection as a known person.[41] It therefore remains to be seen if the court in Ireland will uphold this principle and how it will affect online freedoms

[36] See Fred Muwema Vs Facebook Ireland Ltd. No. (2016) 4637P, http://kampalalawmonthly.com/fred-muwema-v-facebook-ireland-ltd-record-no-2016-4637p/

[37] Court orders Facebook to reveal TVO's identity to Muwema, http://www.monitor.co.ug/News/National/Court-orders-Facebook-to-reveal-TVO-s-identity-to-Muwema/688334-3362002-qu4tn7z/index.html

[38] Ugandan lawyer fails in High Court bid to get Facebook to take down alleged defamatory postings, http://www.independent.ie/irish-news/courts/ugandan-lawyer-fails-in-high-court-bid-to-get-facebook-to-take-down-alleged-defamatory-postings-34995340.html

[39] At the time of writing this report the matter between Muwema and Facebook Ltd had not been completed and was expected to come up in the next months.

[40] Government requests (Uganda), https://govtrequests.facebook.com/country/Uganda/2016-H1/#

[41] America Online, Inc. v. Anonymous Publicly Traded Company, 261 Va. 350, 542 S.E.2d 377 (2001) and Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261, 1264 (C.D. Cal. 2001

in Uganda. The case of TVO also presents a challenge for intermediaries for the need to create a balance between promoting anonymity and freedom of expression online while dealing with cyber-related offenses. According to Muwema's lawyers, the case was heard in Dublin as it is where the relevant division of Facebook is based. The lawyers explained: "Facebook users outside the United States and Canada, such as users located in Uganda, enter into an agreement with Facebook Ireland when they register an account to use the Facebook service. This means that any Facebook users outside the United States and Canada who wish to take court proceedings against Facebook must do so in Ireland before the Irish Courts."[42]

4.3 Online Surveillance

Protection from surveillance is provided for under Article 27 of the Constitution which provides that a person has a right to privacy and no person shall be subjected to unlawful search or interference of communication or other correspondences. Over time this right has been suspended through legal and illegal means. Online surveillance in Uganda has been reported in many aspects. The first reports of surveillance were in early 2000s when government was accused of illegally tapping into phone conversations. Government did not accept or deny this; however, during the debate on the Anti-Terrorism Act the Minister for Security then noted that government had been tapping conversations of persons believed to be engaged in terror activities.[43] In 2006 President Museveni, in a speech to parliament, hinted on a fact that government had tapped into a phone conversation between some MPs and the Lord's Resistance Army (LRA) rebel leaders. Later that year, then-Attorney General Amama Mbabazi while addressing the NRM caucus said they had been illegally tapping into phone conversations and other communication systems for security purposes and was proposing a law to make such a form of surveillance legal.[44] This was the birth of the Regulation of Interception of Communications Act which today is the main law governing surveillance in Uganda.

In 2015, Privacy International released a report detailing how a UK firm Gamma International had allegedly sold spyware to the government of Uganda to help authorities conduct surveillance on the media and political activists. The report alleges that government installed the spyware in public places such as hotels.[45] Whereas government of Uganda denied that it had acquired and installed such spyware, there is growing fear that the government is illegally tapping into communications. Some critics also believe that recent government provision of free internet in Kampala and Entebbe could be a ploy to target government critics by tapping into their conversations considering access to the service requires an individual to register their name, date and place of birth.[46] This same requirement applies during SIM card registration where subscribers are required to provide their personal details. However, the absence of a data protection law is worrisome to some Ugandans who believe that government is misusing all this data to monitor their communications.

---

[42] Muwema V Facebook, http://www.lavellesolicitors.ie/muwema-v-facebook/

[43] For example some of the conversations tapped in early 2006 has been lined up as evidence to be used against former LRA commander Dominic Ongwen facing trial at the ICC.

[44] Telecoms (2007) Phone-Tapping to be legalized in Uganda? Available at http://www.balancingact-africa.com/news/telecoms_en/4146/phone-tapping-to-be-legalised-in-uganda

[45] Privacy International (2015) For God and My President: State Surveillance In Uganda available at https://privacyinternational.org/sites/default/files/Uganda_Report.pdf

[46] Privacy, Anonymity and Security: My case for free Wi-fi in the city, http://aicartech.com/privacy-anonymity-security-case-free-wi-fi-city/

In July 2015, reports emerged that the Uganda Police and the Office of the Presidency were in advanced stages of acquiring hi-tech surveillance software from Israel and Italy to begin large-scale spying.[47] 48 Information released by Wikileaks showed email exchanges between the Italian surveillance malware vendor Hacking Team and its local vendor Zakiruddin Chowdhury, who seemed to have strong contacts with senior Uganda government officials.[49] It was suggested that the LGBTI community could be among the key targets of surveillance.[50] Earlier, in April 2014 after the Anti-Homosexuality Bill was signed into law, the LGBTI community in Uganda was reportedly targeted by Zeus, a spyware which steals confidential information from computers. This law was later annulled by the constitutional court.

4.4 Internet Activism and propaganda

Over the years Uganda has seen an increase in internet-based campaigns including communications and discussion from government officials, discussions among human rights activists, sharing of political information and general discussions. Perhaps the most trending activism on Uganda was the #Kony2012 campaign that involved creating awareness about atrocities committed by the LRA rebel group. [51]

Political activism has involved campaigns by citizens and activists, but often it has seen political leaders engaging with citizens through use of social media. A common method of engagement has been on Twitter sessions under hashtags such as #AskThePM created during former Prime Minister Amama Mbabazi's reign between 2012 and 2014. Other sessions under the hashtags #AskSevo #AskIGP, and #AskIGG were organised to ask the president, the Inspector General of Police and the Inspector General of Government respectively but these did not involve much discussion and were largely ignored by the intended participants.

Social media played an enabling role for candidates in the 2016 elections as they used platforms such as Twitter, Facebook and YouTube to seek direct engagement with voters, promote their online image and solicit for votes. Citizens also took to Twitter to engage and follow electioneering events. For instance, analysis of Twitter activity during the presidential debates using the hashtag #UGDebate16 shows wide engagement by individual activists and by the media, as well as the adoption of automated accounts (Bots) to dominate online discourse.[52] On elections eve and elections day, the alleged Bots were markedly absent from online conversations, likely due to the social media shutdown. Further, during this two-day period, there was a recorded shift in the online emotional sentiment from a positive one to one characterised by suspicion, anger and disgust.[53]

---

[47] Police in Shs 5bn spy deal, The Observer Uganda, http://observer.ug/news-headlines/38889-police-in-shs-5bn-spy-deal

[49] Wikeleaks (2015), The Hacking Team - Re: R: I: Uganda Police, https://wikileaks.org/hackingteam/emails/emailid/11829

[50] Buzzfeed, Emails Reveal Israeli And Italian Companies' Role In Government Spying, http://www.buzzfeed.com/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy#.alWw9nveDK

[51] Kony2012 Campaign was an online activism campaign by an NGO Invisible Children that sought support to carry out activities aimed at arresting the leader of a rebel group Lord's Resistance Army (LRA) that has for over 30 years engaged in war with Uganda People's Defense Forces. The group is accused of carrying out rape, child slavery and marriages among other atrocities.

[52] Analysis of Twitter Activity During the 2016 Presidential Debates in Uganda, http://cipesa.org/?wpfb_dl=210

[53] Analysis of Twitter Activity During Election Eve and Election Day in Uganda, http://cipesa.org/?wpfb_dl=216

5. Conclusion and Recommendations

Generally in 2016 Uganda used legal and non-legal means to limit internet freedoms. A number of laws have been made to curtail media freedoms, many of which appear to target persons critical of government. Some of the non-legal means such as blockage of social media and demand for media personalities to stop appearing on particular programs have been challenged in courts of law. Some respondents felt that the various laws enacted by Uganda in recent years may not necessarily have an immediate effect on use of internet but provide huge potential for curtailing media freedom and internet freedom. Gerald Businge, a media trainer and blogger, said the fact that there is high-level selective application of the law means that such laws are likely to be used against individuals considered critical of government. He said one effect of such laws was self-censorship that is practiced by some internet activists in Uganda.

The current legislation gives broad powers to the communications regulator in regulating the ICT sector. This was seen when UCC ordered ISPs to block access to social media sites and claimed the law gave the regulator such powers. Besides, the Uganda government seems to be using laws to limit internet freedom especially where users are likely to be critical of the state.

Proposed amendment to the Communications Act could be taken as an attempt to give UCC leeway to easily make restrictive regulations without going through parliamentary oversight or control. The Bill tabled in parliament does away with the requirement to present subsidiary legislation before parliament. It also removes powers of parliament to veto such laws.[54]

The current trend in abusing legislation to control internet freedom is likely to continue in the coming years and this may have a negative impact on internet use in Uganda. However, Uganda citizens are fighting back through digital activism condemning government actions and calling for the respect of freedom of expression, assembly, the right to privacy and the right to access information.

Several recommendations are made to different actors as below:

5.1 Government

- There is need to review laws that limit internet freedoms in Uganda and in their place provide for progressive laws that make it easy to use internet securely and openly.
- Government should immediately enact the Data Protection and Privacy law taking into account submissions by stakeholders on vague, weak and regressive provisions.
- The opportunities for mass surveillance by the state should be reduced to guard against infringement on citizen privacy and potential abuse of information.
- There is need for increased investment in internet and related platforms to ease access to information and affordable internet for citizens in Uganda.

5.2 Civil Society Organisations (CSOs)

- CSOs should advocate for the respect for internet freedom by both government, service providers and individuals through increased awareness creation on internet freedom concerns.
- There is need for increased capacity building on the part of government and citizens to enable secure use of the internet.

[54] See the Uganda Communications (amendment) Bill, 2016

5.3 Service providers

- Service providers should challenge government requests that violate internet freedoms by being more transparent in their dealings with the government.

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) under the OpenNet Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa. As part of the project, we are documenting internet rights violations, reviewing cyber security policies and how they affect internet freedoms, promoting information availability and conducting awareness-raising.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
156-158 Mutesa II Road, 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