Unwanted Witness

Amplifying voices Changing lives

AN **OPEN, FREE** AND **SECURE INTERNET:**

A THREAT TO UGANDA'S NATIONAL SECURITY?

AN OPEN, FREE AND SECURE INTERNET:

A THREAT TO UGANDA'S NATIONAL SECURITY?

CONTENTS

1.0	Introduction	4
2.0	Research Methodology	7
3.0	Findings and discussions	8
3.1	Legal barriers to online expression and privacy	8
3.2	Online attacks and threats on Freedom of Expression and Privacy	16
3.2.1	Online Violence against women	16
3.2.2	Online Surveillance and Interception of Communication	17
3.2.3	Cybercrimes	21
3.2.4	Cyber bullying and attacks	23
4.0	Conclusions – Impact on freedom of Expression and Privacy	24
5.0	Recommendations	25

1.0 INTRODUCTION

The Internet has opened up new possibilities for the realization of the right to freedom of expression. This is due to the Internet's unique characteristics, including 'its speed, worldwide reach and relative anonymity'. These distinctive features have enabled individuals to use the Internet to disseminate information in 'real time', and to mobilise people[1]

Unlike any other medium the Internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole[2]. We now have people who are able to express themselves using their own tools, without needing anyone's permission because of the Internet[3].

Online communication in Uganda has been on the rise in the last decade, making Uganda one of the first countries in sub-Saharan Africa to gain full Internet connectivity[4]. Several Internet Service Providers are offering wireless broadband access, and the introduction of UTL's Freenet service and a special Internet tariff countrywide have helped to increase Internet usage, as has the recent strong growth of the fixed-line networks and an explosion of the number of cybercafés[5].

Uganda also became the first country on the continent where the number of mobile subscribers passed the number of fixed-line users, and the ratio is now more than 18:1. Internet penetration stands now stands at 31% of the

1 https://www.humanrights.gov.au/publications/background-paper-human-rights-cyberspace/3-freedom-expression-and-internet
2 Ibid
3 Interview with Charles Mwanguhya – Bureau Chief, the East African
4 http://www.internetworldstats.com/af/ug.htm
5 Ibid

population[6]. Just like everywhere else, the Internet has come to hold enormous potential for development, providing an unprecedented volume of resources for information and knowledge and opens up new opportunities for expression and participation[7].

Although Uganda's Constitution provides for the rights to freedom of expression, including that of the media[8], the right of access to information[9], and the right to privacy[10], rights holders including civil society and media practitioners have come under growing threat by government seeking to restrict citizen voices critical of state operations, through recent laws and regulations, as well as proposed laws in the pretext of protecting "national security"[11].

Across the continent, Internet shutdowns have become control mechanisms governments are using to curtail the right to freedom of expression and access to information online. In addition, many state and non-state actors are steadily moving to curtail what individuals may do online, thereby inhibiting freedom of expression and the right to privacy[12].

The safety and security of the online community has thus increasingly become an issue of concern for many human rights defenders, as groups as well as individuals. This is because the internet has been viewed as an enabler of other human rights, as well as a catalyst for development.

However, in order to embark on responsible and effective programing that will guarantee an enabling, safe and secure operating environment for the online community, it is important to have an understanding of the key safety and security concerns, including triggers and the key factors that facility these

6 Ibid
7 http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/
8 Article 29(1)
9 Article 41
10 Article 27
11 http://cipesa.org/?wpfb_dl=225
12 Ibid

threats and risks, by both state and non-state actors.

This report therefore (seeks to) provides a trends analysis of the existing online safety and security concerns and their impact on the rights to freedom of expression, access to information and privacy, and by extension, other fundamental human rights and freedoms.

2.0 Research Methodology

The research was conducted over a period of 100 days, between the months of January and April 2017, with the primary objective of assessing the state of online safety and security in Uganda, and its impact on peoples' enjoyment of their right to freedom of expression, access to information and privacy.

The study comprised a literature review of key policy documents and publications, including relevant studies, research and media reports touching on the issues of online expression, safety and security in Uganda; including international human rights instruments.

Data was also collected through interviews of staff media and human rights organizations as well as individuals working on issues of online expression, access to information and privacy and data protection in Uganda.

In terms of scope, the study examined a number of areas, including;

- The role of the internet in fostering freedom of expression and privacy;
- Existing legal and policy frameworks that threaten online expression in Uganda; although some laws apply both off and online – defamation, libel, etc.
- The state of online safety and security in Uganda, including the trends of threats and risks;
- Other existing government exertions used to infringe on online communication and free expression
- Impact of online threats and attacks on freedom of expression and privacy

3.0 Findings and discussions

3.1 Legal barriers to online expression and privacy

The rights to privacy[1] and freedom of opinion and expression[2] have been expressly provided for in both universal and regional human rights instruments and interpreted by treaty bodies and regional courts among others.

In Uganda, the Constitution has also provided for these rights; right to freedom of expression and the media[3], the right of access to information[4], and the right to privacy.[5] Over the last few years however, there are a number of laws and policies whose spirits and letter serve to undermine these constitutional guarantees. In many of these legal provisions, the government has fronted "national security" as the basis for curtailing peoples' freedom to enjoy their rights to freedom of expression online.

In 2011, the government passed the Computer Misuse Act[6], to provide for the safety and security of electronic transactions and information systems and to prevent unlawful access, abuse or misuse of information system among other things. However, 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.[7] One of the commonly used sections employed by the state is section 25 of the act, which criminalizes "offensive communication" thus;

1 Article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, among others
2 Article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights, article 9 of the African Charter on Human and Peoples' Rights,
3 Article 29(1) Uganda Constitution
4 Article 41 Uganda Constitution
5 Article 27 Uganda Constitution
6 http://www.ulii.org/ug/legislation/act/2015/2-6
7 CIPESA (2016) The state of Internet Freedom in Uganda

> *"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 twenty four currency points or imprisonment not exceeding one year or both"*

In March 2017, Makerere University research fellow, Dr. Stella Nyanzi first summoned to the Police criminal investigations department (CID) and questioned over cyber offences[8]. She was later to be arrested and charged with two counts under the Computer Misuse Act – cyber harassment under sections 24(1)2(a) and offensive communication under section 25.[9]

According to the charge sheet, Dr. Nyanzi is alleged to have used a computer to post on her social media account content suggesting that his excellence the President, Museveni as a "pair of buttocks"; as well as other offensive messages with the intention of disturbing the peace and privacy of President Museveni. However, Nyanzi isn't the only person charged with offensive communication.

On 31st September 2017, journalists Stanley Ndawula and Robert Ndawula proprietors of an online publication, the investigator were arrested for publishing an article alleging that Inspector General of police Gen. Kale Kayihura had resorted to killing his own police officers as a way of covering up for crime. The duo was charged with offensive communication and liable under the penal code act, the case is still before the magistrate court.

8 http://www.monitor.co.ug/News/National/Dr-Stella-Nyanzi-appear-CID-cyber-crimes/688334-3837538-vfh189/index.html

9 http://www.aljazeera.com/news/2017/04/academic-stella-nyanzi-charged-cyber-harassment-170410183134831.html

Hardly two months later, five (5) Red pepper directors and three (3) editors were arrested following police raid on the head offices. Arinaitwe Rugyendo, Richard Tusiime, Patrick Mugumya, Johnson Musinguzi, James Mujuni, Ben Byarabaha, Francis Tumusiime and Richard Kintu were all charged with offensive communication and Treason for publishing a story deemed prejudicial to national security. After being granted bail, the group met with President Museveni and had charges against them dropped by the Director of Public Prosecution.

In 2015, online activists, Shaka Robert was arrested and charged with "offensive communication, under section 25 of the Computer Misuse Act. Mr. Shaka is alleged to have posted offensive comments against President Museveni about his health.[10]

In December 2016, a political activist, Swaibu Gwogyolonga, was also charged and is still battling charges of offensive communication. Gwogyolonga is said to have posted on his Facebook wall expressing how he will announce and mourn the death of President Yoweri Museveni when that happens. The post was accompanied with a Photoshop of Museveni and how would look after his death.[11]

In 2010, the government had enacted the Regulation of Interception of Communications Act[12] (commonly referred to as the phone tapping law) which is probably the most problematic law when it comes to stifling the Internet freedom of Ugandan citizens. Section 3 of the Act provides for the establishment of a Monitoring Centre for the interception of communications under the Act. It is above all the minister responsible for security who is mainly responsible for establishing and running the centre.

10 http://www.voanews.com/a/social-media-critic-arrested-in-uganda-/2820626.html
11 http://www.chimpreports.com/case-of-man-who-wants-museveni-dead-pushed-to-january-25/
12 http://www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

By enacting this law, the government effectively legalized the interception and monitoring of communications in the course of their transmission through a telecommunication, postal or any other related service or system, contravening the constitutional provision of the person's right to privacy.

Under the law, communication service providers are required to ensure that they are capable to enable the interception of communications at all times or when so required by installing hardware and software facilities and devices[13]. A failure to do this can result in a maximum prison sentence of five years. This provision threatens both privacy and freedom of expression on Internet as service providers, faced with the threat of criminal sanctions are forced to above all take to account the state's interests, not the individuals' interest to be able to enjoy their human rights.

The other legal barrier to online freedom and right to privacy is the 2002 Anti-Terrorism Act[14] which has provision allowing for obtaining information in respect of acts of terrorism, which include the authorising of the interception of the correspondence of and the surveillance of persons suspected to be planning or to be involved in acts of terrorism. These provisions constitute a violation of right to privacy on the Internet, when digital communications are intercepted. The Act also includes provisions that threaten the freedom of expression.

The Act provides that any person who, without establishing or runs an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates news and materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death[15].

13 Section 8, Regulation of Interception of Communications Act 2010
14 http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf
15 Section 9(2)

In 2016, Doreen Biira, a journalists working with a Kenyan-based media, KTN was arrested and charged with "abetting terrorism" under section 9(b) of the Anti-terrorism act 2002[16]. According to the media reports, the Rwenzori Regional Police spokesperson said that Ms. Biira was arrested while illegally filming military activities which media have been restricted to cover on camera.[17] Once convicted, the charge carries a maximum sentence of death.

The term terrorism has also not been properly defined, leaving its parameters so elastic that the provisions of the law can be exploited to prefer any charges against an individual, group or organization.[18]

In April 2017, parliament also passed the proposed Anti-terrorism amendment Bill 2017[19], amending the definitions of "terrorism" and "acts of terrorism. However, the proposal to amend section 2(1), granting the Minister discretional powers to designate a "suspect terrorist" was defeated[20]. This was the third time that the law was being amended, having been amended in 2015 and 2016[21].
Other laws affecting the right to online freedom of expression and privacy and that have been discussed extensively include – the Anti-Pornography Act 2014, which criminalises the production, trafficking, publishing, broadcasting, procuring, importing or exporting and abetting any form of pornographic materials.[22]

In December 2014, musician Jemimah Kansiime and her producer, Didi Mugisha became the first victim to be charged under the law for "willfully and unlawfully producing, trafficking, importing, exporting, selling and abetting

16 http://www.monitor.co.ug/News/National/Kasese-clashes-KTN-journalist-terrorism/688334-3468084-5xnl8u/index.html
17 http://www.monitor.co.ug/News/National/Kasese-clashes-KTN-journalist-terrorism/688334-3468084-5xnl8u/index.html
18 Kimumwe (2014) Media Regulation and Practice in Uganda: A Journalist's handbook
19 http://parliamentwatch.ug/wp-content/uploads/2017/03/Anti-TerrorismAmendment-Bill-2017.pdf
20 https://unwantedwitness.or.ug/government-loses-key-clause-as-parliament-passes-the-anti-terrorism-amendment-bill-2017/
21 Ibid
22 Section 3(1) of the Anti Pornography Act 2014

pornography"[23] for her music video, Nkulinze (I am waiting for you).
Internet Service Providers (ISPs) are also required, not to allow their protocols and systems to be used for publishing pornography[24]. The ISPs have an obligation to monitor and carry out surveillance on their customers if they are to identify and remove content considered pornographic.[25]

Another law affecting freedom of expression, especially for public servants is the more than 50 year old Official Secrets Act Cap 302, of 1964, that criminalizes the collection, recording, publishing or communicating "any secret official code word, or password or any sketch, plan, model, article or not or other document or information which is calculated to be or might be or is intended to directly or indirectly useful to a foreign power". The law has been effective in gagging the public servants as they can be prosecuted for going against the oath of secrecy.

The Penal Code Act, particularly section 176[26], which criminalises libel also poses a great threat to online freedom of expression. In the 2013 matter of Uganda Vs Nyakahuma Kalyegira, Justice Lameck Mukasa ruled that "publication online can constitute a commission of an offence under section 179 of the Penal code Act".[27]

In April 2017, parliament finally passed the contentious Uganda Communications Commission Amendment Bill 2016[28], which effectively expunged parliamentary oversight on the regulations made by the minister. In the proposed bill, the minister had sought the repeal of the phrase "with approval of parliament" from section 93(1) of the Act[29] which read;

23 https://mg.co.za/article/2014-12-11-antiporn-law-screws-risque-singer
24 Section 17
25 CIPESA (2016) State of Internet Freedom in Uganda
26 Any person who, by print, writing, painting, effigy or by any means otherwise than solely by gesture, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, commits the misdemeanor termed libel
27 http://www.ulii.org/ug/judgment/high-court-criminal-division/2013/30-0
28 http://www.chimpreports.com/parliament-passes-communications-amendment-bill/
29 http://chapterfouruganda.com/sites/default/files/downloads/The-Uganda-Communications-Amendment-Bill-2016.pdf

"The Minister may, after consultation with the Authority and with the approval of Parliament, by statutory instrument, make regulations for better carrying into effect the provisions of this Act."

By passing the proposed amendments, parliament effectively elevated the powers of the minister in the control and management of the communication with the mandate to formulate and implement tyrannical or arbitrary regulations that serves his or her interests without any parliamentary oversight.[30]
Even without the amendment, the Act already gives sweeping powers to the minister as well as the Uganda Communications Commission to regulate, monitor and to conduct communication surveillance of citizens' communications across all communications/ expression platforms including the internet[31].

The Communications Act also pays lip service to the notion of independence for the Commission, as the Commission is required to report to and receive policy directions from the Minister of Information and Communications Technology. The Minister is also responsible for appointing the majority of the members of the Board of the Commission, has the power to remove members and retains control over the Board's finances, all of which runs counter to international better practice. These problems are particularly troubling in light of instances where the Commission has targeted critics of government policy. For example, in 2009 four stations were shut down allegedly for discouraging a government-proposed land law.

The Act and its Schedule 4 also include vague rules on content, prohibiting content which is against public morality or which creates public insecurity, while requiring programs to be balanced and to ensure harmony
For many internet and online users, the provisions of these laws are a drawback to their enjoyment of the rights to freedom of expression, including the media and that of privacy – especially during their communication. Many people

30 https://hrnjuganda.org/?page_id=2639
31 https://www.unwantedwitness.or.ug/internet-they-are-coming-for-it-too.pdf

are fearful and become guarded on what they post online and thus do not communicate freely.[32]

Recommendation

The government should consider amending all the above laws and policies that criminalise freedom of expression and also give broad powers to both the minister and law enforcement agencies and be replaced with provisions that promote and protect citizens' online freedoms and privacy.

Specifically,

Section 19 under the Anti-Terrorism Act should specify the circumstances in which each type of surveillance and investigation is appropriate to safeguard adherence to the principles of necessity and proportionality; Also, any order for the interception of communications under Section 19 must explicitly require judicial authorization;

In regards to the Regulation of Interception of Communications Act; the definition of "national security of Uganda" in Section 1 must be more narrowly and precisely defined to avoid arbitrary interpretation and application by authorities; Also, the procedures for the judicial authorization of interception warrants must be made explicit in Section 5 to ensure interceptions are truly necessary and always proportionate.

With regards to the Anti-Pornography Act; The definition of "pornography" in Section 2 should be redefined with greater precision to limit the scope of representations that are criminalized and prevent the suppression of legitimate forms of expression, discrimination against women, and undue restriction of cultural practices; Additionally; Section 11 should be struck in its entirety to prevent ISPs from bearing responsibility for accessing and distributing illegal content.

32 Interview with Isaac Imaka, Journalist Daily Monitor and Chair, Uganda Parliamentary Press Association

3.2 Online attacks and threats on Freedom of Expression and Privacy

In Africa, many governments have tended to establish surveillance mechanisms to monitor the online communications of their citizens. Online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression force individuals around the world to seek security to hold opinions without interference and seek, receive and impart information and ideas of all kinds.

3.2.1 Online Violence against women

Just like the offline gender-based harassment, there are clear gender differences in the cyber bullying and harassment itself against men and women. While the men are to a larger extent attacked for their opinions, women receive nasty comments and attacks that are related to their gender and appearance.[33]

In 2015, the media reported incidents of 7 girls in Uganda who were alleged to have been raped by strangers they had met on facebook[34]. According to the reports, one of the girls was raped following her post on Facebook, saying she was looking for someone to help her achieve her dream career of modelling. The unsuspecting girl received a barrage of responses and was hoodwinked by one persuasive response by a man who promised to not only fund but also connect her with renowned models.[35]

Incidents of revenge porn targeting women have been registered in Uganda where women's private information, including nude pictures and videos, are published on social media without their consent[36]. Unfortunately, the victims who have included musician Desire Luzinda[37] and television personalities Anita Fabiola and Sanyu Mweruka, were further subjected to threats of prosecution under the Anti-Pornography law instead of pursuing the perpetrators

33 http://sciencenordic.com/young-women-twice-exposed-cyber-bullying-men
34 http://www.monitor.co.ug/News/National/7-girls-raped-via-Facebook-in-one-month/-/688334/2898628/-/70wt64z/-/index.html
35 Ibid
36 http://www.cipesa.org/?wpfb_dl=209
37 http://www.monitor.co.ug/News/National/Desire-Luzinda-should-be-locked-up-and-isolated--Lokodo/688334-2510248-e7ukrg/index.html

responsible for the uploading of the video.[38]

Online violence against women in the form of revenge pornography is on the increase, and their emails are intercepted or hacked into to obtain images that are eventually used for blackmail[39].

It may be hard to establish the extent of online violence against women since most women do not report for fear of reprisals and counter-accusations, or lacked the knowledge of where to report and seek redress.[40] Majority of women are now reportedly scared of speaking or engaging in online communication, which impacts on their ability to fully enjoy their right to freedom of expression.

3.2.2 Online Surveillance and Interception of Communication

The passage of the Regulation of Interception of Communications Act in 2010, marked a low point for digital rights in Uganda. The law effectively erased the notion of and the right to privacy of communication as enshrined in Article 27 of the Constitution. Since then, the government has been in overdrive to monitor, and intercept peoples' communication.

In 2014, the Uganda police was reported to have set up the cybercrimes unit, "with the intention of fighting cybercrimes", and had its staff trained by foreign experts in monitoring cybercrimes.[41] The move was however criticized by human rights activists as an attempt by the government to find avenues of infringing on its citizens' rights to privacy and expression.

In 2015, an investigative report by Privacy International (PI) blew the cover of a secret operation, code named Fungua Macho, where the government is said to have bought an intrusion malware FinFisher from Gamma International GmbH ('Gamma'). According to the report, the malware was used to infect communications devices of key opposition leaders, media and establishment

38 http://www.monitor.co.ug/OpEd/Commentary/Sex-tapes-are-part-of-pervasive-levels-of-violence-against-women/-/689364/2618598/-/q4h7kiz/-/index.html

39 Interview with Rosebell Kagumire, online activist

40 http://cipesa.org/2015/10/the-challenge-of-tackling-online-violence-against-women-in-africa/

41 http://www.monitor.co.ug/News/National/Activists-cry-foul-as-police-set-up-cyber-crime-unit/688334-2249294-r8ixtjz/index.html

insiders over period between 2011 and 2013.[42]

The report further noted that covert FinFisher's access points in form of Local Area Networks (LAN) were installed within Parliament and key government institutions. Actual and suspected government opponents were targeted in their homes. Hotels in Kampala, Entebbe and Masaka were also compromised to facilitate infection of targets' devices.[43] Fake LANs and wireless hotspots were set up in apartment estates and neighborhoods where many wealthy Ugandans and expatriates live.[44]

Once infected, a person's computer or phone could be remotely monitored in real time. Activities on the device become visible. Passwords, files, microphones and cameras can be viewed and manipulated without the target's knowledge.[45]

The government has also been active in disabling peoples' online freedom of expression by ordering ISPs to effect internet shutdowns, including other online transactions such as mobile money transfers. During the elections in February 2016, the government banned social media on Election Day with the president defending the decision as a "security measure."[46] For large parts of the day, people were unable to tweet, use facebook and other social media platforms including Whatsapp,[47] although a few managed to use alternative routes, and applications such as VPN to bypass the blockade.[48] The impact had however been massive as majority of people who rely on the mobile money platforms to transact their business were affected[49], and those who rely on social media for information were also affected.

42 https://www.defenddefenders.org/wp-content/uploads/2016/03/The-Right-to-Privacy-in-Uganda-Uganda.pdf
43 https://www.privacyinternational.org/node/656
44 Ibid
45 https://privacyinternational.org/sites/default/files/Uganda_Report.pdf
46 http://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/
47 http://www.monitor.co.ug/News/National/Social-media-Mobile-Money-switched-off-over/688334-3082556-fnl4xjz/index.html
48 http://www.dignited.com/16837/ugandans-use-these-apps-to-access-blocked-whatsapp-facebook-twitter/
49 http://www.cgap.org/blog/impact-shutting-down-mobile-money-uganda

Unfortunately, the practice continued during the swearing in ceremony in May 2016, when once again social media platforms were blocked[50].

It is important to note that attempts by the state to shutdown online communication are not new. In 2011, as the country was preparing for the presidential and parliamentary elections, the government is reported to have instructed telecom companies to block short message services (SMS) that contained key words like; "Egypt", "people power" among others.[51] Additionally, one of the mobile telephone company MTN was blamed for jamming and blocking the telephone lines that the opposition party, Forum for Democratic Change (FDC) had bought for its agents to assist in the transmission and tallying of election results. The telephone company denied the allegations[52].

In 2011 still, after the hugely contested elections, during the "walk-to-work" protests orchestrated by the opposition, the government was again reported to have asked ISPs to shut down facebook and twitter for at least 24 hours[53]. The government had also banned live coverage of the protests by the main stream media[54].

In March 2013, the Uganda Communications Commission announced the implementation of the mandatory countrywide SIM card registration exercise, with mobile subscribers required to register with their mobile operators[55]. The exercises was criticised and challenged in the courts of law over; "alleged illegalities, irregularities and anomalies in the exercise[56]. As provided for under section 9 of the Regulations of the Interception of Communications Act, telecom companies were required to obtain personal information, such as the person's full name, residential address, business address, postal address and his or her identity number contained in his or her identity document.

50 http://allafrica.com/stories/201605130317.html
51 http://af.reuters.com/article/topNews/idAFJOE71G0M520110217
52 http://telecomafrica.blogspot.ug/2011/03/ugandas-opposition-calls-for-mtn.html
53 http://www.monitor.co.ug/News/National/-/688334/1147082/-/c2o6bqz/-/index.html
54 http://www.monitor.co.ug/News/National/-/688334/1147082/-/c2o6bqz/-/index.html
55 https://ugandaradionetwork.com/story/telecom-operators-cagey-on-number-of-registered-simcards
56 http://www.biztechafrica.com/article/uganda-sim-reg-be-challenged-court/5300/

In the absence of privacy and data protection law or policy, the exercise raised a lot of concerns among citizens on the safety and security of their data in the hands of telecom companies.

There have also been questions marks on the government's objective of pushing ahead with the exercise – fighting crimes; with many experts opining that there is little evidence that the registration has had any effect on the rate of cybercrime[57].

Indeed, after a spate of murders and killings, mobile phone subscribers were given 7 days to re-register their SIM cards with telecom companies or risk having their lines de-activated. Unlike before, the only documents permitted for the exercise were the national IDs for Ugandans, passports for foreigners and certified registration documents from the office of the Prime Minister for refugees.[58] And yet this contradicts the provision of the Regulations of Interception of Communications Act and the regulations that provide forms of identities and no specifically the national identity card nor passport[59]. Unfortunately, in order to enforce the directive, the telecom companies were given access to personal confidential data captured during the national ID registration exercise[60].

In August 2016, the Minister for Ethics and Integrity, Fr. Simon Lokodo, announced that the government had contracted a South Korean company to supply the pornography detection machine. According to media reports, the machine had the capacity to detect porn pictures, videos, or graphics taken or saved on one's phone, computer or camera in any form[61].

57 http://www.itwebafrica.com/ict-and-governance/400-uganda/237652-analyst-says-sim-card-registration-in-uganda-is-ill-advised
58 http://www.monitor.co.ug/News/National/UCC-gives-phone-users-7-days-to-register-afresh/688334-3886696-ncfkxoz/index.html
59 https://drive.google.com/file/d/0BxywtPsTqJdocmhqcjREaXFrRkE/view
60 http://allafrica.com/stories/201704020199.html
61 http://www.newvision.co.ug/new_vision/news/1431545/pornography-detection-machine-arrives-august-lokodo?utm_source=dlvr.it&utm_medium=twitter

Additionally, courts of law have developed a habit of entertained telephone call print-outs as evidences from either government or a private person without questioning the processes under which such information was acquired. For instance; Criminal Case No. 1488 of 2009: Uganda Vs Juliet Katusiime, David Sebuliba & Major Godfrey Kyomuhendo the Magistrate Court sitting at City Hall in Kampala; heard that Juliet Katusiime was frequently communicating with her brother Godfrey Kyomuhendo and relative Mohammed Kateregga and David Sebuliba. This was evidence submitted as telephone print- outs from the telecommunication operators without considering how they prosecution got such evidence without a court order to tap a citizens communication. The phone call print-out was however accepted by the trial magistrate as key evidence to convict and sentence Katusiime to a 3 year jail term[62]

3.2.3 Cybercrimes

Although the Internet and other digital technologies have profound value to the rights to privacy, expression and opinion, they have also tended to offer governments, corporations, criminals and pranksters unprecedented capacity to interfere with these rights, including that of privacy[63].

In 2016, it was reported that sophisticated crimes like computer and credit card fraud were becoming more frequent, and there was worry that identity theft would follow shortly[64]. The Uganda Communications Commission reported to have recorded 200 cyber related cases in 2016 alone[65].

According to the Uganda Police Bi-annual crime report (January-June 2015), there had been an increase in the number of registered cases from 61 in 2014 to 137 (more than 100%) over the same period[66]. Banks and other financial institutions were at the biggest risk of cybercrimes with many cyber criminals

62 https://www.unwantedwitness.or.ug/internet-they-are-coming-for-it-too.pdf
63 Kaye, David (2015) UN Special Rapporteur on FoE
64 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19707
65 https://www.independent.co.ug/200-cyber-related-crime-cases-reported-uganda-2016/
66 http://www.mediacentre.go.ug/sites/default/files/rescrc/BI-ANNUAL%20-%202015%20%5BCompatibility%20Mode%5D.pdf

targeting mobile money and online banking services.[67] According to the African Cyber Security Report 2016, Uganda's financial institutions lost about $35 millions in cybercrime.[68]

According to the Uganda Police[69]; between the month of August and November 2014 only, mobile money frauds caused a loss of over 207 million UGX (80,000 USD)[70] to the users. Within the same year, ATM/VISA frauds led to a loss of over 1.2 billion UGX (460,000 USD) from over 700 victims by use of scheming devices installed onto ATMs located in Kampala and other areas

Cyber-criminals have proven to be relentless and greatly improved the level of sophistication of their attack methods with an increasing focus on obtaining sensitive information supported by the emergence of virtual currencies.[71] In Uganda, many Internet users are heavily reliant on their ISPs to provide them with some level of security, although the more sophisticated users tend to have additional security through use of anti-viruses, passwords and firewalls[72]. There are a number of threats and risks involving personal computer security, impersonation especially on social media.[73] And yet it is believed that Cyber-crime instances are mainly discussed socially and the victims suffer in silence, while the perpetrators continually hide under the invisibility of the cyber world[74]

According to experts, many Uganda are prone to cyber-crimes and attacks due to their limited knowledge and skills[75] on how to navigate the murky waters of online transactions and weak safety and protection infrastructure in place[76].

67 http://allafrica.com/stories/201508190908.html
68 http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
69 http://www.upf.go.ug/cyber-barometer/
70 The USD/UGX exchange rate then was 1USD=2500UGX
71 https://www.nita.go.ug/media/cyber-threat-horizon-uganda-2016
72 https://www.itu.int/osg/spu/cybersecurity/contributions/Uganda_Bugaba_paper.pdf
73 Interview with Louis Jadwong, New Vision
74 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.8447&rep=rep1&type=pdf
75 Interview with Edrine Wanyama, CIPESA
76 http://www.monitor.co.ug/Business/Technology/Uganda-at-risk-of-cyber-crime--experts-warn/688612-3348368-if44eq/index.html

In 2014, the National Information Technology Authority established the national Computer Emergency Response Team (CERT) to protect the nation's internet infrastructure, as well as coordinate responses to and defence against cyber-attacks.[77] However, despite these developments, the police's ability to conduct forensic analysis on devices and trace cybercrimes is still rudimentary and that the police and investigative agencies often turn to private forensic experts to assist in the complex investigations[78].

3.2.4 Cyber bullying and attacks

As noted earlier, the universality of the Internet has created an online community which presents a double edged sword to the uses. Due to the massive excitement to share, online users are sharing large volumes of personal information, and unfortunately, this information is increasingly being used against them by cyberbullies, stalkers criminals, with some cases leading to crimes such as kidnapping.[79]

In April 2017, journalist and writer, Uwitware Getrude was kidnapped at gunpoint and held captive for hours. During the hostage, Uwitware says her abductors threatened to kill her for her views and thoughts, which she had shared on her blog[80] about the controversial Dr. Stella Nyanzi. Uwitware reported to have received online threats before the abduction.[81]

Many other online users are however prone to cyber-attacks due to their naivety and lack of skills and knowledge to protect their communication, including the more personal data. Only a few are aware of the risks and threats that online users get exposed to, but the majority are not aware.[82]

77 https://www.nita.go.ug/media/nita-u-launches-national-computer-emergency-response-teamcoordination-centre
78 https://www.privacyinternational.org/node/965
79 http://www.theeastafrican.co.ke/business/Cyber-criminals-bleeding-Africa-financial-institutions-dry-/2560-3505564-item-1-fay3n5z/index.html
80 https://trudiz.wordpress.com/2017/04/02/stella-nyanzi-only-did-what-we-have-feared-to-do/
81 https://cpj.org/2017/04/ugandan-journalist-abducted-assaulted.php
82 Interview with Patrick Tumwine - HURINET

4.0 Conclusions – Impact on freedom of Expression and Privacy

From the above findings, it is clear that despite the growth of internet subscription and literacy levels, the right to online freedom of expression and privacy is still a major challenge for the majority of internet users in Uganda due to the high levels of threats and attacks, including online surveillance.
Despite the constitutional guarantees of the right to freedom of expression, access to information and privacy, Uganda has continued to pass laws that contain retrogressive provisions with a negative effects on these rights. Laws such as the Computer Misuse Act, Regulation of Interception of Communications Act are often used to arrest and charge online users.

Violence against women, especially revenge porn has been on the increase with many women being threatened with blackmail and attacked. This has led many women to hold back on their level of online communication and living in fear of having their intimate data exposed or used against them.
It is also clear that the government has intensified its surveillance machinery through the cyber-crimes units, and invoking the RICA and other laws such as the computer misuse act to charge online communication.

Peoples' right to privacy has also been compromised a lot by the on-going mandatory SIM card registration exercises, and yet there is no privacy and data protection law/policy that will oblige agencies collecting and storing personal data to protect and keep them.

There is also an increase in the wave of cybercrimes and attacks targeting online users. These have ended up having a chilling effect on peoples' enthusiasm to fully engage in online communication and transactions, thus limiting their ability to enjoy the benefits, including enhanced opportunities to enjoy their fundamental human rights.

5.0 Recommendations

Government

Government should expedite the process of enacting and implementation of the privacy and data protection law, to safeguard peoples' private and personal data being held by the various individuals and agents who have collected it in the course of the SIM card registration, medical/health visits and academic undertakings among others

Government functionaries/agencies that are not anchored in law and transparent, such as the cybercrimes unit of the police, social media monitoring units, among others should be scrapped and replaced by legally bound entities that are transparent and accountable

Civil society

Key civil society actors should work to hold the government accountable to promote and protect her citizens' online freedoms of expression and privacy, as provided for in the Constitution and other international human rights instruments

Whenever possible, actors – civil society, individuals and ISPs should challenge government actions in the courts of law as a way of promoting respect for the rule of law.

Ordinary citizens

Citizens should equip themselves with the right tools and skills to circumvent government and other non-state actors' surveillances, by encrypting their communications and online transactions and avoid falling prey to cyber-attacks, crime and fraudsters.

Media

The media should undertake investigative approaches to their reporting by putting the government to task to explain their actions and they (media) should also provide their audiences the right kind of information.

ISPs

Internet and other communication service providers should question and actively participate in the legislative processes as well as challenge retrogressive laws that impede on peoples' right to online freedoms of expression and privacy.

Plot 41 Gaddafi Road. P.O.Box 71314 Clock Tower K'la
Tel: +256 414 697 635
Email: info@unwantedwitness.or.ug
www.unwantedwitness.or.ug
Unwantedwitness-Uganda
@unwantedwitness
unwantedwitness