THE INTERNET:

THEY ARE COMING FOR IT TOO!

Unwanted Witness
Amplifying voices Changing lives

Hivos
people unlimited

With Support From HIVOS

THE INTERNET:
THEY ARE COMING FOR IT TOO!

With Support From HIVOS

JANUARY 2014

THE INTERNET

THEY ARE COMING FOR IT TOO!

TABLE OF CONTENTS

AKNOWLEDGMENT

Unwanted Witness Uganda greatly appreciates the Ministry of ICT, UCC and National Information Technology Authority (NITA-Ug) for providing relevant information regarding internet security and safety risk in Uganda. Special thanks goes to the Bloggers, HRDs, artists and other related individuals for being forthcoming and providing information that was the basis of the study.

We thank Ms. Suzan Ombaru and her technical team for their tireless efforts in putting together the bits and pieces of this assignment. Her support and mobilization of partners for active involvement is greatly appreciated. We further thank the entire staff and research assistants at The Unwanted Witness who dedicated their time and efforts to collect the important information.

Our final words of appreciation go to HIVOs for their moral and financial support to the study.

Unwanted Witness Uganda

Management

ACRONYMS & ABBREVIATIONS

HRDs	Human Rights Defenders
UCC	Uganda Communication Commission
NITA-U	National Information Technology Authority- Uganda
ICT	Information communication Technology
ISOC	Internet Society
UN	United Nations
CBOs	Community Based Organizations
CSOs	Civil Society Organizations
NGOs	Non-Governmental Organizations
MDAs	Ministries Districts Agencies
IT	Information Technology
CISO	Computer Information Systems Oracle
ISPs	Internet Service Providers
CMI	Criminal Management Investigation
UPF	Uganda Police Force
GBV	Gender Based Violence
UDHR	Universal Declaration of Human Rights
4GC	For God and my Country

EXECUTIVE SUMMARY

This report sheds more light on why digital rights and internet freedoms should be protected, under a study commissioned by Unwanted Witness Uganda. Internet use is steadily growing as penetration increases; the new wave of increased activity by Ugandans online is evident. This is attributed to the penetration of mobile telecommunication companies that have closed the internet divide across the region, geographical location, gender access and utilization.

During the late 90s and early 2000s, internet access was limited to urban centers, with the rural areas relying on traditional forms of media like radio and word of mouth. This was majorly because the internet had been confined to the profiting urban centers and at the various town internet cafes. With the emergence of mobile internet, the availability of smart phones on the market and with increased investments in telecommunication infrastructure, many of the rural areas got connected on the net.

This has been matched with the enactment of various laws termed Cyber Laws that govern the internet. These cyber laws aim at regulating the access and use of the various internet related platforms. These actors have noted aims at controlling other than facilitating the enjoyment of freedoms of expression, speech, association, assembly and access to information online which rights are not only guaranteed by the 1995 constitution of the republic of Uganda but also provided under various international human rights instruments to which Uganda is party to.

The introduction of 3G and mobile internet has increased quick, easy and reliable connection onto the internet. A number of Ugandans now access and utilize the internet mainly through social media platforms like facebook, Twitter, WhatsApp, Yahoo and Gmail among others. But while we celebrate all this, many Ugandans are not yet on board majorly due to the high access and utilization costs, and the lack of knowledge.

The few who are utilizing the internet have been conducting various activities from business, expression or networking among others. This has come as a result of the increased censorship currently experienced under the traditional main stream media with continued unabated curtailment and clump down by various government agencies with actions ranging from threats to suspend licenses, controlling access for certain sections of the public to expression platforms, filtering content, to recommending the dismissal staff or employees deemed critical of the political establishment.

The many activists who are otherwise denied access to the said traditional media have found solace in the invention of the internet especially the various social media platforms as medium of expression and new workplaces. That notwithstanding, the choice of platforms has not kept them safe from the long arm of the state.

It's from this backdrop that the Unwanted Witness Uganda an internet based advocacy civil society organization undertook a protracted research aimed at understanding internet security and safety risk in Uganda. The study respondents comprised of the various government regulatory institutions and individual citizens; netizens; bloggers; poets; artists; HRDs; freelancer writers among others in order to bolster their safety and security while working online.

The findings indicate minimal threats; especially due to the ignorance by activists of the existence of the said threats and lack of capacity to determine the type and nature of threats. This is matched with technical capacity building initiatives currently being implemented among the various government agencies that aim at working to threaten the enjoyment of online freedoms through massive surveillance and snooping. To do this the government has established a social media monitoring centre, constituted an internet unit within the Uganda police force and passed/ developed social media regulations for civil servants to engage with the public online. These and much more are signs of an orchestrated campaign designed to safeguard the status quo by the government and limit the full utilization, access and enjoyment of various internet freedoms or digital rights.

While Internet freedom connotes the access and use of the internet without control, censorship, limitation or restrictions for any reason that may be, a critical analysis of legal frame that governs internet security and safety in Uganda. Threats have been majorly indentified on the basis of access and unitization that has enabled E-Participation in the implementation of human rights advocacy issues and mobilization of citizens to participate in policy reforms through online debates. Internet reliability highlights internet irregularities faced by online activists with occasionally internet network interruption during demonstrations. Internet security, issues of insecurity indentified at national and individual levels were attributed to lack of information on internet security by users and less emphasis put by the regulatory bodies to create awareness on internet security. Online environment; users felt insecure and there was increased insecurity particularly noted among was fear to express sensitive political issues.

The extent of Internet censorship varies from one situation-to another though being moderate, government has gone as far as requesting for FaceBook to disclose certain information of some citizens on the social media platforms under the disguise of national security and criminal investigations. The findings suggest that government seeks to address the gaps in the regulatory bodies, and while there is need to enact the data protection, surveillance and privacy law and seriously implementing them to ensure the right to privacy of different online users are guarantee, and e-Government regulations through massive awareness creation and capacity building to support more online services and participation.

SECTION 1: INTRODUCTION

Background

The government of Uganda established the Uganda Communication Commission and National information Authority- Uganda as the agencies of the government to oversee; regulate communication and develop the IT infrastructure among others. Various legislations such as the Computer Misuse Act 2010, Electronic Transaction Act 2011, the regulation of Interception of Communications Act; The NITA Act 2009; The UCRA Act 2012 and the UCC Act among others were enacted to provide for the use, security, facilitation and regulation of electronic communications and transactions to encourage the use of e-government services and to provide for such related matters.

The UN Human Right Council Resolution on the promotion, protection and enjoyment on the internet A/HRC/20/L.13, recognizes that the internet is a universal space for communication and the exchange of ideas that can promote freedom and mutual understanding among all people, regardless of race, religion, geography or economic status. As a result international organizations, civil society organizations (HRDs), individuals/artists and government ministries have adopted the use of online services as the fastest avenue to express themselves, transact business and share information through the different plat forms, thus increasing social, academic, economic, religious and political participation of citizens, HRDs, CBOs, national and international CSOs and government to promote democracy and good governance.

Considering that there are some particular situations where the use of Internet is under a grave and gathering threat, with imprisoned political dissidents, activists and bloggers are always in urgent need of protection. While the UN internet freedom declaration therefore affirms that: Everyone has the right to equal access to the Internet, regardless of race, religion, ethnic or geographical origin. Everyone has the right to the free flow of information and freedom of expression without fear of discrimination. Any attempt to restrict or intimidate people from free, uncensored, and secure access of the Internet constitutes a fundamental abridgement of human rights and undermines the promotion of peace and world order.

On the other hand its alleged by various government internet regulatory agencies, that internet freedoms have been misused in one way or the other as many individuals/ organizations have gained unauthorized access to citizens personal data, security password to defraud government ministries, individuals, and banks, identity threats, website defacement and email scan.

Situational analysis of internet safety and security in Uganda

Over the past few years the security ramifications of online activities have begun to permeate the national consciousness. However, despite the growing level of interest in this field, there is still little known about the actual issues involved in securing networks and electronic assets (NISS, 2011). Internet information safety and security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It is in this regard that the Ministry of Information and Communications Technology whose mandate is to provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy in all matters of ICT in consultation with various stakeholders has drafted a National Information Security Strategy 2011 as part of the national cyber security to address the information security issues at national level.

IT information skills vary from entity to entity. Lack of knowledge in some institutions results into hiring of IT services to: - install, implement or update IT systems without much emphasis on information security. There are currently few Ministries, Districts and Agencies with information security strategies or policies. The absence of top management support and too little financial support in implementing information security measures is also prevalent among many MDAs.

Currently, there are ways in which the Uganda government has designed to address the risks associated with information security in a knowledge based economy

First of all the government developed Strategy Frameworks such as incorporation of IT issues in national development plans e.g. The National Development Plan (2010) under objectives, strategies and interventions, section 328, objective 2, strategy 1, which calls for the enhancement of use and application of ICT services in business and service delivery. This requires a national information security strategy in order to safeguard the use and application of ICT services in service delivery.

Secondly the draft National IT policy (2010) for Uganda under the IT Security objective, strategy 1; calls for development of the National Information Security Strategy. Among other laws and regulations developed to regulate IT activities with the country not limited to only service delivery but accomplish also personal, NGO works like advocacy on human rights, blogging and use by activists.

On the other hand in order to ready itself, the government through NITA has been undertaking series of trainings to build capacity within MDAs in monitoring and management of computer security incidents and the execution of proper responses to those incidents, which is important to develop a well understood and predictable response to damaging events and computer intrusions.

Despite presence of these policies, trainings on cyber security, laws and regulations, many Ugandans lack relevant information on computer and internet use and are not sure of the safety and security of their online information related to political, social, and democratic governance issues. This is directly linked to the fact that internet freedom in Uganda is not very free to guarantee access and utilization of internet based platforms as medium of freedom of expression which is provided for in the Constitution of Uganda. According to the 2012-13 Annual Freedom report, Uganda's rankings on freedom on the net was described as being partly free[1]

Purpose and Objective of the study

The purpose of the study is to understand the internet safety and security threats in Uganda faced by HRDs online, and to inform the appropriate support to victims, address security capacity gaps amongst HRDs, foster collaborations/partnership among national, regional and international actors and governments, as a way of influencing a secure and accessible internet to all users for quality debates, opinions and thoughts among others. The overall study objective was to bolster the safety and security of artists, activists, bloggers, netizens and freelance journalists while utilizing new digital media technologies to strengthen and guarantee the enjoyment of freedoms of; thought, speech and expression, in Uganda.

[1] Freedom House (2013); Freedom on the Net, A global Assessment of Internet and Digital Media

Specific Objectives

1. To establish a deeper understanding of safety and security risks and threats faced by HRDs through research.
2. Address security capacity gaps among artists, bloggers, Netizen and freelance journalists in utilizing both online and offline safety and security tools and measures to guarantee their safety
3. Establish collaborations to defend and promote digital rights and internet freedoms in Uganda through emergence response support to HRDs to continue with their work online.

Methodology

Sample selection

The respondents were purposively selected and presumed to be having knowledge on internet safety and security. Interviews were conducted with key officials in the ministry of ICT, NITA-UG, UCC, Civil society organizations, individuals basing on their knowledge on internet safety and security and daily use of online services. In addition, individual artists, activists, bloggers, poets, and netizen who ordinarily use the internet as a means of expression were also interviewed. The majority of the interviews were conducted using English. Researchers employed open ended questionnaire guide in order to ensure that the questions require more than a one or two word response and an inviting quality that will encourage authentic responses and two-way communication in both personal and professional relationships between research assistants and the respondent.

Data collection methods

The study relied on the use of qualitative research methods, an approach that offered the opportunity to explore deeply the perceptions of internet security and safety based on personal experience, and to investigate the ways in which improvements to their plight could be made. The data collection methods used included: key informant Interviews and document reviews;

Key Informant Interviews: KII were conducted with the help of KII guides. Questions were drafted to cover specific themes relating to online services and security and safety and were modified where appropriate.Three (3) KIIs were held at national level with UCC, ICT and NITA-Uganda. KIIs were also held with HRDs, Bloggers, Netizens and freelance journalists and artists.

Document Reviews: These were conducted on key policy related issues on internet security and safety to give contextual analysis of the existing laws and regulations that guide online activism, and identify gaps in information to be filled during primary data collection. A multi-disciplinary team reviewed documents and reports related to internet safety and security in promoting good governance in Uganda. These included studies, publications and global literature reviews of internet safety and security. There data on on-line internet use was available from different organizations such freedom House (Freedom on the net), ICT policies, UCC guidelines among others.

Data Processing and Analysis

Data was transcribed within 24 hours after every interview by each research assistant. The transcripts produced were edited and harmonized for completeness, accuracy, readability and meaningfulness under the lead consultant. Data was then word processed and analyzed by theme and content with the help of computer assisted software (Atlas ti).

Ethical considerations

Before conducting any interview, respondents consent to be interviewed was sought by the research assistant. This was very important to make sure that they willingly gave information and were not coerced and to ensure that their values, cultural norms and beliefs were put in to consideration and never tempered with. The purpose and objectives of the study were clearly explained to the respondents before carrying out the interviews. Respondents were assured that the information they shared was to be kept confidential and nobody will be identified with any information since these will be grouped with responses from other respondents.

SECTION 2: FINDINGS

2.1. Digital Rights and Internet Freedoms: Why they should be protected?

The term internet freedom connotes the access and use of the internet without control, censorship, limitation or restrictions for any reason that may be.

The United Nations Human Rights Council has noted in its resolution that internet freedom is a basic human right and that people have the right to freedom of expression on the internet.

The council sitting on June 28th 2012 guided by the UN charter passed resolution A/HRC/20/L.13 for the promotion, protection and enjoyment of human rights on the Internet.

That the exercise of human rights, in particular the right to freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies. And further took note of the reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to Affirm that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights; and Called upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;

While Internet access provides for online freedom of expression as basic human right, it also stands as a source of information, news and provides platforms where individuals can express their thoughts, opinion and views, calling for the need to keep it free and unrestricted for the enjoyment of such rights ordinarily enjoyed offline, especially freedom of expression that has no frontiers. Freedom of the internet is a human right whose importance will only increase in today's knowledge society and be achieved only if it is left free from censorship.

On the other hand, civil society organizations such as Unwanted Witness Uganda under the Internet Rights and Principles Coalition have developed guiding principles termed as the Charter of Human Rights and Principles for the Internet. The purpose of the charter is to provide a recognizable framework anchored in human rights for upholding and advancing human rights for the online environment. The goal breaks down into 3 main objectives viz;

1. To provide a reference point for dialogue and cooperation between different stakeholder priorities for the internet's design, access and use around the world.
2. An authoritative document that can frame policy decisions and emerging rights based norms for the local, national and global dimensions of internet governance
3. A policy making and advocacy tool for governments businesses and civil society groups committed to developing rights based principles for the internet.

Below are the principles[2];

LEGALITY: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative Act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

LEGITIMATE AIM: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

NECESSITY: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least

[2] https://en.necessaryandproportionate.org/text access on the 11th January 2014

likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

ADEQUACY: Any instance of communications surveillance authorised by law must be appropriate to fulfill the specific legitimate aim identified.

PROPORTIONALITY: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. There is a high degree of probability that a serious crime has been or will be committed;
2. Evidence of such a crime would be obtained by accessing the protected information sought;
3. Other available less invasive investigative techniques have been exhausted;
4. Information accessed will be confined to that reasonably relevant crime alleged and any excess information collected will be promptly destroyed or returned; and
5. Information is accessed only by the specified authority and used for the purpose for which authorization was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority that:

1. Other available less invasive investigative techniques have been considered;
2. Information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3. Information is accessed only by the specified authority and used for the purpose for which was authorization was given.

COMPETENT JUDICIAL AUTHORITY: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. Separate from the authorities conducting communications surveillance;
2. Conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3. Have adequate resources in exercising the functions assigned to them.

DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law[3] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.

USER NOTIFICATION: Individuals should be notified of a decision authorizing communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the surveillance is authorized, or there is an imminent risk of danger to human life; or
2. Authorization to delay notification is granted by the competent judicial authority at the time that authorization for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give

[3] The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

TRANSPARENCY: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance[4].Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the

[4] The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinize the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See http://www.iocco-uk.info/sections.asp?sectionID=2&type=top.

identification of users as a precondition for service provision[5].

SAFEGUARDS FOR INTERNATIONAL COOPERATION: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a Foreign Service provider. Accordingly, the Mutual Legal Assistance Treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

Unwanted Witness Uganda believes democratic governance is about an established relationship between the state and the citizens. A basic requirement for such a relationship is an informed citizenry which relies on media and other communication platforms such as the new age digital platforms to receive information and engage in debate passing on their views and opinions. Through the media especially the various web based digital platforms now, citizens are informed of their leader's actions and performance and comments are ascertained.

The internet provides a number of diverse expression platforms that the Unwanted Witness Uganda believes should be kept unrestricted at all costs for the enjoyment of

[5] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.

such rights ordinarily enjoyed offline, especially freedom of expression, opinion and thought as it provides new boundaries without frontiers. Bearing in mind that Article 19 of the Universal Declaration of Human rights provides guarantees for the protection of expression noting that; *“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”*

The internet has become the center of freedom of expression and considered as the pillar of rights as it provides various platforms where the expression takes. However, current trends in the country say otherwise. As Uganda seeks to position itself to use ICT as the backbone for development especially driven by Vision 2040, in addition the increase in internet penetration and use within the next few decades will witness many people seeking to access the internet and hence expression platforms.

While the increasing internet penetration and use is viewed as a positive development, it is equally matched by continued fears of increased resort by political establishments to sophisticated and legal restrictions to limit citizens’ access and use of the internet and its expression platforms. This ordinarily means an impediment to the enjoyment of internet rights and freedoms.

The methods of restriction have included, low band width and slow speed, massive surveillance, blocking of sites and the passage of cyber laws or application of existing ones, to restrict user anonymity, restricting user privacy and monitoring general free expression online by serializing comments of participants. This has been strengthened by the establishment of the social media monitoring center that aims at monitoring various internet based social platforms.

The above among others provide the biggest challenges still facing the enjoyment of internet freedom especially internet access in Uganda. Its uneven distribution greatly affects access and utilization. With many people in urban centers having access regularly, little or nothing much has been done to reduce the disparity in the rural areas. The gaps are not only related to lack of infrastructure, but also, knowledge and skill. Rural areas not only have limited access to electricity, but also internet services. Very few if any internet cafes do exist in rural Uganda hence limiting access. While in the urban areas many people utilize the access provided by their mobile telephone service providers to through mobile internet.

The protests that marked the 2011 irregular general elections and the rising cost of living drew many people on the streets, with information about the protests being shared across various internet based platforms. The effect was an order from the Uganda Communications Commission directing ISP holders to deactivate and censor social platforms. To that end many activists could not log onto their accounts on the various social platforms. This trend has gone on unabated and whenever the country is experiencing protests termed by the authorities as riots, internet access becomes restricted where some activists fail to access their social platform accounts.

Hence the Unwanted Witness Uganda through the digital rights programmatic intervention will seek to defend and promote online freedoms to prevent unabated surveillance, restrictions and increase opportunities for greater access and utilization of the internet among citizens to fully enjoy their internet freedoms while keeping in mind their safety and security and the enjoyment of the right to privacy while online.

The Internet Legal Framework in Uganda

Like any other freedoms enunciated in the Universal Declaration for Human Rights (UDHR), Internet Freedoms too are provided for and protected as other rights. Specifically mindful of Article 19 of the UDHR that provides; *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."* The internet has been argued as forming the other frontiers envisaged under the UDHR.

Whereas the1995 Constitution of the Republic of Uganda does not explicitly guarantee internet freedoms but does provide for under Article 29 the protection of freedom of expression, Expression as noted either connotes the right to freely speak out regardless of frontier to which the internet is among. The notion of seeking, 'receiving and imparting information and ideas through any media and regardless of frontiers' has been construed to include the internet. That, while individuals have rights offline such rights cannot be derogated whenever they are online.

Uganda is currently positioning itself to control how digital freedoms should be exercised. Such actions are witnessed by new legislations that give legal force to the establishment and transaction of business via the internet. For a long time the access and use of the internet had not been legislated against by any national or domestic laws until at the close of 2010 when the government enacted a number of legislations termed ‘cyber laws’ aimed at governing and regulating activities done via the internet including transactions, communications and expression among others. Many of these legislations have passed unchecked and implemented with very little monitoring including the regulations for interception of Communications Act, the Computer Misuse Act, the Electronic Signatures’ Act, the Electronic Transaction Act, the Anti-Pornography Act, the NITA Act and Uganda Communication Authority Act; the Social media Regulations among others.

The National Information Technology Authority Act 2009

Established in 2009, NITA Uganda is the body mandated under the NITA Act to oversee the driving of information technology in Uganda. The authority aims at providing high quality informational technology. Since its establishment, NITA has spear headed the enactment of various laws that comprise of the legal framework governing internet in Uganda, it is also working to establish the necessary infrastructure that may enable all Ugandans to access and utilize information technology. This has enabled a substantial number of persons in Uganda to connect to the internet.

NITA has also been at the fore front in overseeing the development and enactment of various policies like; The e-government policy; The e-government strategy; and The IT policy which give the operational framework through which government IT infrastructure operates.

The Uganda Communications Act 2012

The Act establishes the Uganda Communications Commission as a body corporate. UCC is responsible for the establishment of the legal framework that enables communications. Among other duties, UCC is the regulatory body responsible for regulating communications, licensing broadcasters, monitoring the implementation of the all laws concerning communication.

However, various actors are concerned that UCC is seen as a stooge used by politicians especially the government to limit and regulate information dissemination platforms. Many actors with opinions that are not in conformity with government are increasingly being denied such platforms. UCC is also responsible for the implementation of the interception of communication regulations which law aims at ensuring surveillance of all communications in Uganda.

The Act under S5 provides the functions of the Commission among others under S5 (1)(b) to monitor, inspect, license, supervise, control and regulate communications services. And in subsection (j) to receive, investigate and arbitrate complaints relating to communications services, and take necessary action; and in (u) to establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators. The commission has used the latter to establish the Social Media monitoring center and the interception of Communication monitoring center under the regulation of interception of Communication Act to conduct communication surveillance of citizens' communications across all communications/ expression platforms including the internet.

a) The electronic transactions Act 2011 and The electronic signatures Act 2011

The Acts aim at the regulation of security of electronic transactions and devices, and providing legal regulations for the use of electronic signatures, and criminalize unauthorized access. Until recent, Uganda had been declared as an internet free state with no known restrictions or limitations on what is viewed or shared.

b) The Computer Miss-use Act 2011

The Act aims at establishing offences related to the use of computers. It provides for offences related to sending messages via any electronic device like a computers that are threatening, and may create fear for life of the recipient including stalking. The Act aims at preventing further what is considered as unlawful access, misuse of information systems through computers and electronic devices basically focusing on limiting child pornography, those posting such material and the intended users. The Ministry of ICT under the Computer Misuse Act 2011 seeks to address online child safety, they have taken on online awareness creation and sensitization through partners like ISOC Uganda chapter on child pornography. Under this program numerous schools have been visited to create awareness

c) The Regulations for the Interception of Communications Act 2010

The law provides power to the minister of security with a court order to intercept any communications in Uganda. It was enacted as an aftermath of the 2010 Kampala terrorist bombings. The law has been used as the legal framework which requires all SIM card holders to register and seeks to order all communication service providers to ensure that their systems enable the interception of communications by the monitoring center. This its argued aims at unfairly and without any regulation breach privacy rights of persons by interfering with their communications contrary to Article

27 of the 1995 Constitution of the Republic of Uganda and various international human rights instruments.

Despite the government operationalizing the different laws that regulates internet activities which under the broad title cyber laws the research revealed that the respondents interviewed had inadequate knowledge on the legal frame work that governs internet use in Uganda. There were very few respondents who have ever heard about the laws from friends but were unable to cite a clause or section from the laws.

Only one respondent from UCC reported having participated in the formulation of the laws. However, the majority of the respondents interviewed are ignorant on the specific laws and their contents, for example those who never heard about the legal frame work attributed it to lack of awareness, poor consultation and on the other hand those consulted never got any feedback from the government especially the key internet providers and users, moreover interestingly for "those" who claimed to know the law, they were not sure of the contents that regulate internet activities , this can be evidenced from one respondent who had this to say;

"No, but I think I looked at the Electronic Act or the e-Bill I have forgotten what it is called but it must be the electronic act not the interception thing, no." This clearly indicted the respondents' ignorance of the existing laws and raises the question of who then can know how the legal frame works? Above all despite the laws established to regulate internet activities, on the other hand it is likely that government has ever taken any initiative to sensitize its citizens on these laws.

The study further showed that though the government has embraced e-government and conducting online activities, different organizations on the other hand have their own internal procedures that regulate on- line service use within the organization for instance Makerere University online service is accessible during working hours, other organizations limits downloading and use of very big files, and others permit the use of online service in regards to organization activities.

The above legal framework provides the country with enough legislation to monitor all communications done on whatever frontiers including the internet notwithstanding however, is that that there is no specific law governing internet use in Uganda.

Using the various said cyber laws, the government institutions have been able to monitor and threaten with closure such service providers who do not filter internet posts by users. This was witnessed especially during the various times whenever the country was embroiled in demonstrations or protests. This action is one which authorities deem necessary to limit the spread of information as protesters/ 'Rioters' used the social media platforms to recruit, re-guide and re-enforce. These actions can be said to constitute threats to internet freedom in Uganda and were the reasons for the establishment of the social media monitoring center and the enactment of the social media regulation policy.

However, recent developments have witnessed systematic build up by government agencies to consider shutting down or limiting internet freedom. In 2010, a blogger Timothy Kalyegira was the first known person to be charged of offences relating to internet expression. This case has dragged on since with the courts failing to decide as to whether the statements made via the internet constituted an offence there being no known legislation to give effect to the same.

The UCC Act also gives the government permission to tap into personal communications deemed to be a threat to national security. This action can be requested by the Minister for Security and granted after an order by a High Court Judge. In effect, the Act provides undue powers to state organs to intercept private communications and potentially threatens free expression through the restriction of content and access to information.

Some media observers worry that the Act *"will likely embolden the government to go after online work more aggressively. It will snoop around more, hacking into people's emails in the name of ensuring national security[6]."*

Unwanted Witness Uganda, through its Digital Rights and Internet Freedoms program do promote the use of cyber space as the primary platform and defend it for purposes of not being gagged. Ensuring that access to the various expression platforms/ frontiers is not restricted and aims at protecting through provision of both legal and psychological supports to activists whose freedoms are being threatened.

[6] Freedom on the Net 2013

Access and Utilization of online Expression Platforms

In Uganda, internet accessibility and utilization is estimated at close to 6 million, with only 2.7 million having active internet accounts[7]. According to the regulator, the Uganda Communications Commission (UCC), the entry of new service providers and increased capacity investment in broadband by operators have resulted in increased internet penetration and changes in the methods of access to internet. Most Ugandans access the internet/online services through their mobile phones. With 850,200 mobile phones and 84,558 fixed internet subscribers and the cost of bandwidth coming down, the numbers are bound to continue growing in the coming years.

The study revealed that the majority of the respondents easily access and use online expression platforms, with many respondents saying it's a key component that encourages high level of engagement among the different category of organizations, bloggers and individuals that constantly use the different online service platforms such as the social networking medium like Facebook, Twitter, Instagram, Google+, Yahoo, Gmail, Hot mail among others to express themselves on social, political and economic issues in respect to the kind of work they are engaged in. For instance, one key respondent described how accessible and easy utilization of on-line services is. *"I use internet quite often, actually I would say if I would be awake 24 hours, I would be using Internet 24/7 but sometimes I get to sleep but so long as I am awake, am either on internet on my laptop or on my phone. Yeah"* Another respondent acknowledged that *"because of many portals from which I can access internet around my work place, internet access is very easy.There is both wired and wireless connection so, one is always connected".* Another respondent from an IT Company described internet as an essential component in life, and said that he cannot live without it.

2.4. Internet Reliability

Constant Internet reliability is a key global network, which links individuals, governments and organizations with similar objectives to promote good governance and fundamental human rights, through online activism. The research findings showed that occasionally there are irregularities in internet reliability, sometimes the internet is slow, however respondents noted that they were not contented with the service providers; they explained the following as some of the factors associated with internet not being reliable.

[7] John Nasasira (2013) :The Global e-government forum

Service providers having “special” links with government thus regulating service providers on internet provision, especially during riots and protest, online networks are constantly interrupted. This further was noted by a respondent that during the 2011 election the opposition party alleged that the phone company MTN had sabotaged its tally centre by jamming the telephone lines of its polling station agents, thereby making it impossible for them to transmit results. The party called for a boycott of MTN services. MTN has the biggest number of subscribers of all operators in Uganda.

On the other hand a key informant explained internet reliability varied from one location to another , he said, *“internet in Kampala is pretty reliable/ stable and as you move further out of the city, if you go to the villages, if you go up northern Uganda, if you went to Busia it becomes a bit stingy but within city centers Kampala, Jinja ,Mbale, it is pretty much reliable that explains why online participation is low in upcountry areas in regards to governance, social and political debates*“.

2.5. E-Participation

The study further established that, the kind of work/activism varied from one person to another depending on the nature of the work. Some respondent’s reported using online services for human rights advocacy and human rights capacity building, campaigns, following news websites and organizations website, while others developed website/ web systems to market their activities online, mobilization of Ugandans for a social, economic and political cause especially HRDs, on issues such as anti-corruption and other development related work.

In addition both private sectors and government agencies have taken to online banking to facilitate the private business, payments of salaries, M-track decentralised reporting system in government ministries.

Following the numerous online expression platforms, with respect to internet activism, the findings showed opened doors for online participation and expression among HRDs, CSOs, International NGOs, government bodies and journalists, and bloggers gradually adopted the use of online expression platforms to advocate for and create awareness to promote good governance, many of them have developed and created online quorum for individuals to participate in key social, political and economic issues affecting them and sensitising citizens to demand for accountability and fight corruption at all levels from the grass root to the top, campaign on social issues like domestic violence, GBV, human rights abuse at different levels in the communities.

Activism on internet has to some extent been successful. For example a key informant described blogging as a chief promoter of his journalism career. He testified about his success that he attributed to blogging as "*well I have been working online as a blogger for a long time since 2006, by then I was working as a reporter with a newspaper company. As a junior reporter, it was not easy to have a social media platform like Facebook to express opinions. My routine work was about discovering a story and reporting it but I realized that I needed a place where I could put my opinions on political, democratic and service delivery issues that I had seen. I decided to open a blog and started writing. I was not very knowledgeable on blogging but my skills improved as I continued as a reporter and blogging at the same time. After 3 years, I got an award, a Journalist Bloggers Award which was run by Global Voices. As a result I got exposed and met on-line working people from Dakar in Senegal in 2009. I learnt and enhanced my writing skills and knew that online work means a lot and that people can be inspired to get engaged in on-line activism and participate in democratic and governance debates*." Another respondent described how blogging can be useful in both private and public work.

"I have been doing a lot of blogging and for the last three years after my Master's Degree. I have been doing my personal work and work for other NGO's, CSOs, CBOs and I participate in online campaigns on domestic violence, human rights abuses, corruption and promoting freedom of expression. I also engage in social issues like mobilizing citizens for social-economic and political debates".

More so the respondents expressed that use of internet for activism is on the rise. One key informant noted that previously most Ugandans used radios and TVs to express their opinions as the only available platforms then. There were programmes called "*Ekimeeza" otherwise known as the People's Parliament at Plot 18, Old Port Bell Road, Kampala, to listen to and engage in public debates on issues that affect them politically, socially and economically in communities. Unfortunately the government closed this programme down, and claimed that some contributors are undermining national values of respect and common decency. Yet these were avenues for citizens to engage in public debates which could result into policy reforms, formulation and encouraged citizen participation in governance issues. Fortunately this happened when the internet penetration was going high and government tries to limit the citizens to express their opinions on open debates. But Ugandans are people who look for a way to express them-selves and the internet has come at a right time where people can freely express themselves.*

For instance, a respondent expressed that "*regardless of restricting open debates and radio talk shows*, *activists couldn't be hosted on radio but now they have a mass following online and they can address people even off radio, like the "Sejjusa letter series" people didn't need to listen to the radio to know what Sejjusa had done, they would go to facebook to see what Sejjusa had posted. It was all over on Facebook even before the newspapers brought it out."*

Respondents continued to argue that activism can be done even through mobilization. A key informant acknowledged the contribution of social media in changing state dynamics. He cited the case of ***the Arab spring*** and how internet changed the countries which all happened in the past 2 years.

"*You know every day people watch revolutions and they couldn't believe that such revolutions would happen anywhere in the Arab world, when someone mentions the Arab spring, then we all think of the social media. I think even before then many Ugandans didn't know what Facebook and didn't know that they could use it. Currently in Uganda there is increasing knowledge on social media platforms use for expression of interest, rights, opinions and advocacy for example a lot of political mobilizations like 4GC used social media to facilitate walk to work campaigns.*

In recent months, regime critics and opposition political parties have taken to the internet as a

Platform for political debate and as an informal means of disseminating information to the masses, that allows citizens to report information and events via SMS texts as they happened. Integrating SMS, online forums, email and Twitter, the platforms attempted to support fair and transparent elections in real time.

In addition, social media has been widely used as a platform for protest in Uganda by providing the exercise of the freedoms of assembly and demonstration otherwise outlawed by the Public Order Management Act 2013, mainly by activist groups. For example, the continuing campaign against the government's proposed give-away of Mabira Forest, Uganda's largest rainforest, to an investor has been sustained partly through SMS, Facebook, and email alerts. The president's proposal to clear parts of the forest to pave way for a sugar plantation is opposed by environmentalists, citizen groups, and some politicians who have used social media to disseminate alerts with key facts about Mabira and the environment in Uganda, and to occasionally call for action and demonstrations[8]

[8] Freedom on the net

2.6. Internet Insecurity

Despite the majority of the respondents interviewed reporting that they access internet quiet frequently, many felt insecure due to internet security, therefore indicated the need to secure internet network. The alarming issue that raised eyebrows among the respondents was limited knowledge on internet security among online service users. Respondents identified several insecurity situations among which included;

- Password sharing commonly cited among organizations and as a result, confidential organization's information is compromised and hacked.
- Personal irresponsibility to protect personal passwords for example a respondent noted incidents where most internet cafe users do not sign out and they ignorantly submit data and detailed information about themselves to unknown sources. Computer/ email hackers at times get hold of such personal information. "The respondent pointed out a situation where a key opposition leader left a flash that had important information at the internet café and also left his information on the desk top where he had worked."

The less effort put by government regulatory bodies to sensitize citizens on internet security awareness, has led to increased cases of cybercrimes that involves wide range of offences, which includes computer data and systems hacking, computer related forgery, fraud and copyright offences faced by internet users, similarly as noted in the findings majority of internet users are unaware of organizations/bodies that handle such insecurity offences, where such crimes can be reported and on what legal grounds.

Further respondents noted threats to right of privacy as one of the core aspects of freedom of expression. For example, voices from respondents in regard to privacy below clearly portray internet insecurity:

"*I fear because I know that photographs can easily be intercepted and privacy is usually easy to intercept e.g. look at some media house printing nude pictures of key people in the country ,yes I mean the right to privacy is under threat. It is very likely that hackers can easily access private information, even at parliament I am quite certain when they want to print my email they do it at ease and indeed they do it*."

"*Your security depends on the ethics of the person who is holding your information for example when you go to a website and submit in your information may be your name, email address and password, it all depends on the terms or privacy terms of the other party that you will be able to know that your secure or not*"

"In any case you are submitting your data to unknown "something" just because you want to achieve a goal, either register and get somewhere or maybe download something, you find yourself putting your information. Usually what drives people is what they are going to get, but they do not think of what would happen to their after. Imagine if Facebook God forbid thought of trading the information they have right now, they would make lots of money, lots of money."

2.7. Internet Security/information gaps

The study revealed a wide gap on information related to internet security both at national level and at individual on-line user level.

At national level, respondents cited less emphasis to sensitize on and regulate internet security laws and policies, because limited information is given to internet users. As noted by some respondents, few were aware of the existence of laws such as Electronic Signature Act, The Computer Misuse Act 2010, Electronic Transaction Act 2011, and lacked knowledge on the contents of these Acts as well as expressed doubt on government's ability to vigilantly implement the laws.

One respondent cited *"I do not think that the regulatory bodies are actually doing anything using the legal frameworks to facilitate/promote internet security information, the government itself is seated with its hands folded. UCC hardly regulates and informs internet users on internet service provider's activities yet some data charges are exploitative and cannot be afforded by the over age and low income earners"*

However, many respondents noted similarly the problems relating to the internet and computer users; having inadequate knowledge on computer usage as another factor for example a key informant noted that among government agencies, work is run by secretaries as he explained. " *they cannot implement, they have internet and they don't know how to use it, they don't know internet…you go to the PS(Permanent Secretary)'s offices and all they know of is a phone call to the reception, but when you send an email they ask their secretaries to read and print for them. I do not think government agencies themselves have taken the initiative to take this up to the next level when it comes to giving information and computer skills".*

The respondents further noted that although there is a police unit called Cyber Police in place to monitor illegal activities such as posting pornographic materials on social media platforms, they are not vigilant enough to curb the ever increasing cybercrimes. “*For example if you are in Uganda posting pornographic material on your Facebook and Twitter it should be illegal because pornography is illegal in this country however our cyber police do not do pretty a good job because they do not monitor such things, we have a lot of pornography sites coming up. A lot of people are using Facebook and Twitter for pornographic purposes and nothing is done about it”,* expressed a Key Informant.

2.8. Online and offline Internet working environment

This is very crucial in promoting/ increasing online participation in decision- making, and advocacy for democracy and human rights freedom by HRDS, bloggers and freelance activists.

The research established that there is on going insecurity in the internet operating environment as the respondents noted that, they always felt insecure especially in expressing sensitive political and human rights issues because the on-line service environment becomes tensed, resulting in the arrest of some rights activists over organized demonstrations , media houses were closed and their online networks connection dismantle. Personal passwords of key individuals/ activists being hacked to monitor their online activities, used to solicit money, and defraud banks, NGOs and government agencies for example a respondent explained how insecure his online environment is and had this to say *“each time I log in, I feel as if someone is monitoring what I am doing. During the Office of the Prime Minister’s (OPM) saga, someone was monitoring the activities within the organization, look at how they got passwords in the finance ministry to transact huge amount of money for their own benefit”.*

Another respondent also said*,” it is not secure at all, people go to cafes punch in their passwords and actually power goes off and you know these computers sometimes store passwords or internet is slow someone gets disgusted and moves out, leaves their passwords in there and anyone can re-log in and actually change their password change the security questions.*

Therefore there is limited awareness across government, private sector and the wider public on the internet operating environment.

The online operating environment is a good model of getting work done compared to off-lines ways of doing things. The world has shifted from paper to digital and firms today are embracing IT operating environment to get work done with high productivity, efficiency and effectiveness. A lot of opportunities have been realized by firms that have had shifts from off line and online platforms; though there are a number of challenges that need to be addressed along these opportunities the challenges are cyber terrorism.

2.9. Digital Democracy in Uganda

The enactment of an ICT Policy in 2003 provided an opportunity for leveraging on ICT in development and governance. The findings of this study showed active media/ online service users both in government agencies and private sector, however freedom of expression still remains a challenge where the government tends to interfere with its citizen's online participation. An example is the recent attempt by the government through UCC asking IPS to block the social media plat forms, because it was argued the social media was mainly used to mobilize activists groups. During the walk to work campaign some internet service providers were temporary blocked and opposition leaders being arrested, and brutally man handled.

2.10. Cyber Censorship

Cyber Censorship still poses as a challenge since it works against democratic freedom of online expression; however the extent of Internet censorship varies from one situation-to another. The study revealed that Uganda being a democratic country, internet censorship is moderate, but of recent, Uganda has gone as far as requesting for Facebook to disclose certain information for six months of some citizens on the social media platforms under the guise of national security and criminal investigations[9].

Furthermore a key informant interviewed had this to say, "Citing the frequent demonstrations and protests by opposition and activists over mismanagement of government funds, harassment of oppositions, police brutality, suppression of freedom of speech and on-line expression, government also requested service providers to temporary block internet and claimed that it would incite the public for more protests." 10According to freedom on the net, the first reported case of internet censorship in

[9] Daily monitor Monday December 2013

[10] Freedom on the net

Uganda occurred in 2006 when the government allegedly blocked access to the news website, RadioKatwe.com, in advance of the presidential and parliamentary elections. The website published content submitted by internet users from all over the world that was critical of the government.

2.11. Data protection, Surveillance and enjoyment of the right to privacy online

The study showed that, with the established regulatory laws, there was no specific law that guaranteed data protection or prohibited surveillance and promoted the right to privacy in Uganda. However a respondent noted that there is indirect surveillance of internet by government and service providers, the respondents were able to note that in situations where government suspects that there may be political riots and protests, security agencies with the complicity of service providers within the country block access to particular sites. They silently chip in to monitor and disorganize online activities of government oppositions and activists.

Another respondent's expressed worries over the rapid trend of SIM card registration for mobile phone users which began in 2012 and noted that this was another method of online service user surveillance and the process requires the mobile user to give detailed bio data information, however this clearly indicates data protection, surveillance and attainment of the right to privacy online is undermined.

Building a strategic surveillance system towards spying on un-ware citizenry

It's now about fifteen years as Ugandans celebrate active use of the internet and the coming of new media. Such development was at first seen as a medium for the elite group (those who knew how to use a computer, read and write and send e-mails) but now it's being appreciated by many as something which is presenting opportunities of multiple medium of communication to achieve development.

After the coming of the mobile phone in the mid 1990s with the launching of Celtel, the first mobile phone service in Uganda, until about 2009 with the arrival on the market of the first Internet-enabled phones, the cell phone and the Internet were two different technologies delivered on different platforms.

It’s estimated that about 14 million Ugandans out of 32 million total population of Uganda is using mobile phones while 6 million Ugandans use internet daily. With the smart phone and later tablet computers, the two have become fused into one gadget which makes internet part of citizens’ lives.

The invention of FaceBook, Twitter and WhatApp whose platforms are mostly used in Uganda, the use of internet and digital gadgets especially mobile phones amongst the citizens mostly the youths has also increased. The new media then which was known for socialization has become a platform to have quality debates on issues concerning citizens ranging from service delivery, governance, accountability, rule of law to citizens discussing how they should be governed.

The shift to use the internet by the citizens occurred after witnessing the endless crack down on the offline media by the government whose actions resulted into the current suffering from high levels of censorship by the traditional media at both institutional (media houses) and individual (practicing journalist) levels.

Despite the challenge of low internet access and speed which stands at 156 mbps among the slowest in the region, citizens as per the current trend view internet as an engine which facilitates enjoyments of rights and freedoms online and foster development.

2006 was seen as a turning point for online freedoms and rights. That year witnessed the growing interests by government to policing and controlling how such freedoms and rights should be enjoyed online especially the right to assemble, association, expression and privacy clearly indicates that the political establishment fears its people.

During that period, the Uganda government made the first move and blocked an online news website called Radio Katwe and track down the people suspected of being behind it. Radio Katwe published highly sensitive reports and news stories about the state, the president and his family and other secret information.

The surveillance journey in Uganda;

In 2007, State House brought in a team of Israeli computer wizards to coach Uganda’s Intelligence security organs on how to; (i) hack into e-mail accounts of individuals perceived to be opponents of government including opposition politicians, human rights activists, journalists and lawyers among others, (ii) carryout forensic investigations on computer hard drives especially those allegedly found in possession of opponents of government and (iii), operate surveillance equipment that monitor both voice and data communications.

Setting up Internet Monitoring Units

Following the coaching process which went beyond 2007, the establishment of Internet Monitoring Units in major security organs took effect.

The same period witnessed the recruitment of ICT graduates in major universities to bridge the capacity gaps.

State House

At State House, Entebbe a counterintelligence desk whose main work is to monitor social media and the Internet has been established and the unit is being headed by an army officer at the rank of a captain.

Although the powers of the unit is still unknown but it recently imported a gadget from the Peoples' Republic of China that has the capacity to monitor ten phone calls at a go.

Sources told this researcher that priority targets are scheduled for surveillance, usually for about a month. If the threat is deemed to have reduced, other targets are selected.

Internal Security Organization (ISO)

The ISO's unit has a bigger team and it reports direct to the Director General of ISO. A committee has to first detect what is likely to happen on the political seen then meet and decide on which phones to be monitored. Any ISO officer who wishes to monitor a particular e-mail account or phone writes to the Director-General of ISO, who then uses his discretion to grant permission or not to the officer.

Also, under this unit all Internet Service Providers and Telecom companies are under obligation to provide, when requested, records of voice and data communication of various people. Since the main servers of some of these companies are outside the country.

Uganda Police Force jumps into the queue to establish its own unit to watch over Internet.

A new unit (the Media Monitoring Unit) within Uganda Police has been established to watch-over online expression Platforms. The Unit is a semi autonomous and the latest to be established after the Media Crimes Department in 2008 within police. The Unit is based at the police headquarters and reports directly to the Inspector General of Police and sometimes to the Police Spokes person's office who then decide the action to be taken against a blogger or any other internet user who might have posted anything deemed critical to the political establishment.

The newly established unit has hired human resource and expertise (IT professionals outsourced from the public) with additional manpower got from within the police force (Cadets graduates of Mass Communication and ICT) and has a structure. Although the unit has not been made public, its structured within the administrative units of the force and receives funds from public coffers through the Inspector General of Police's office.

Despite having the expertise and the structure in the existence, the unit's powers are still unknown. It watches over all online platforms including Face book, Twitter, Blog posts, and LinkedIn among others.

How the Unit got established;

The Unit under the code name "Media Monitoring Unit" was founded in late 2010 the deputy spokes person of police by the then at the rank of Cadet Assistance Supretendant of Police (ASP) to dissect both radio and television programs and news paper articles with intension to counteract anything written or broadcast about the president, police as an institution and the Inspector General of Police. And one of the cases the unit handled upon establishment was a case of a book writer Nzaramba Vincent who was arrested by security operatives and held incommunicado for days over his book PEOPLE POWER – BATTLE THE MIGHTY GENERAL. Until the Prime Minister's office recruited Glenevin Public Relations and security firm from Ireland in 2012 the unit's work was expanded to cover internet monitoring.

Glenevin an Operational Risk and Security Consultancy was hired at a about Shs. 2 billion close to a $ 1 million to offer training to staff of the Government of Uganda to better equip them to actively manage the country's global reputation.

The firm introduced the Uganda Police Force to online media and expanded the then mandate of Media Monitoring Unit to include watching over the internet. Also, the firm opened the official police Face Book Page.

According to a source at the police headquarters told the Unwanted Witness that the firm disbanded the entire unit and set the new rules including but not limited to monitoring the use of all online platforms and the content published, collect "critical" information published online about government and police and share it with the Inspector General of Police for action, provide first hand news about the operations of police on all online platforms and not to wait for traditional media to break such stories and to provide regular responses on posts or stories published online with intention to protect the image of police and government.

However, as the process of enhancing capacity of the internet monitoring team was still ongoing, it came to an abrupt end as the contract with Glenevin had expired and wasn't renewed by the government. This created a half-baked team which resulted into not delivering to the expectation of the government especially the police leadership.

Such situations saw police leadership outsourcing more expertise from the public. To this, two senior journalists were recruited on contract to bridge the existing gap each with separate responsibilities. One of these journalists qualified from a foreign university was decorated with the rank of Assistant Commissioner of Police (ACP) upon recruitment. The said ACP heads the Internet monitoring unit which collects all materials published online and reports directly to the Inspector General of Police. While the other heads the Capacity Building Component at the Media Monitoring Unit. Upon the recruitment this second journalist was too decorated with the rank of Commissioner of Police (CP). The overall job is to train police officers to defend the image of government and police in both online and offline media writing and developing own content.

Although 2013 registered a case in which the government of Uganda made a formal request to the Face Book Company to provide details of a facebook account holder as per the company's report of 2013, but the request was not granted due to insufficient grounds for what they would use such information incase its provided.

The Unwanted Witness findings show that the Police's Internet Monitoring Unit for the past one year has profiled dozens of internet users particularly those deemed to be opponent of government. This happening towards the 2016 general elections one can say internet users specially those who uses it to express their opinion or thought are likely to face a wave of acts of vengeance from government.

Using Telecom Companies to Spy on citizens;

Unwanted Witness notes that the Government is currently using private telecom companies to spy on citizens in total disregard of the constitution especially breaching Article 27 on the right to privacy;

The Genesis of surveillance to privacy

Uganda has experienced the most dramatic development in telecommunications in the last decade where the growth of mobile phone subscribers has grown from less than one million in 2001 to more than 14 million in 2011. Uganda is ranked among the ten African countries with the highest number of mobile phone subscribers.

The country has a host of Mobile Network Operators (MNOs) among whom include MTN Uganda, Orange Uganda, Uganda Telecom, and Airtel among others offering both voice and data communications. However, the increase of mobile subscribers as per the current trend has given government leverage over citizens' private life.

On July 11, 2010 in Kampala, Parliament hurriedly passed the Regulation of Interception of Communications Act, which requires telecommunication companies to install surveillance equipment that enables electronic surveillance of people through their mobile phones without the need of a court order. Thus, making all MNO subscribers terrorism suspects.

The MNOs especially those that have been operating in Uganda for over five years and above have faced undue influence and pressure from government demanding for print-outs of phone calls made by any citizen without court orders. Such print-outs have been used against activists or Human Rights Defenders (HRDs) to justify their arrests, arbitrary detention or at times used as evidence in courts of law.

A case in point is a case of Arafat Nzito a journalist working with one of the radio stations in Kampala. He was kidnapped from his workplace and detained incommunicado for more than six (6) days on grounds that he communicated with someone in an Arabic country.

Nzito then told Unwanted Witness that "Before being kidnapped, I first received calls from someone who claimed that he wanted to give me a story. Little did I know that they were kidnappers. In a few minutes, I was called to move outside the office and meet them in the radio station's parking yard. Upon getting out, I found three officers dressed in plain clothes with a private vehicle. They pushed me into the car and found myself in the middle of two armed men. Immediately, the kidnappers pulled out a phone call print- out demanding for details of the person I was accused of communicating with from an Arabic country. I pleaded my innocence in vain until I was taken to Summit View – Kololo a suburb of Kampala and I was kept in a cave for a number of nights" said Nzito.

He added that he was chained both legs and arms; detained in a small cold and dark room which was too short for him to stand throughout the detention period. Mr. Nzito was later dumped in one of the trading centers without being taken to court to answer any charge.

The mandatory SIM Card registration being enforced under the Regulations of Interception of Communication's Act, 2010 takes more than what is necessary for the process. For re-instance any mobile subscriber is required to provide his/her pass port photo, address for both residence and workplace, next of kin and an identity card among others.

Secondly, the process was being spear-headed by MNOs which responsibility should have been that of the government. The fact that Uganda has no National Information Storage Center where citizens' collected data is stored the right to privacy will continue to be abused and eroded. This means all the data which has been collected will remain in the hands of private telecom companies and subject to abuse.

The SIM Card registration which started late 2012 and ended in August 2013 has been bogged with a reasonable number of irregularities intended to subject citizens to secret surveillance, increase possibilities of telecom companies workers' to access customers' personal data and stifle free speech online.

An artist told the Unwanted Witness that one day he called to complain to the customer care service of one the telecom companies in Uganda however the attendant who picked the call responded by calling his name and mentioned place of his residence. "I felt like someone who's naked whose private life has no protection. This is a total infringement on my right to private. How do those companies that came to do business in Uganda access my private life? I think workers of these telecom companies enjoy unlimited access to our data and listen to our private conversations" said the artist.

The other incident is MNOs tagged terms and conditions on the registration forms which wasn't catered for in the law with one of the telecom company Warid among its terms embedded at the back of the registration form stating that "with or without the permission of the subscriber, the company will hand-over any subscriber's information on the request of the government"

Also, the absence of a Data Protection law to regulate the collection, storage and access to citizens' personal information, their security is endangered regardless of one citizen is in public office or a private citizen since their information can be access by anyone. Under the same law, citizens must exercise control over personal data collected about them and its usage where anyone who requires personal data from person should request the individual's informed consent regarding the content, purposes, storage location, duration and mechanisms for access, retrieval and correction of their personal data.

The Unwanted Witness fears that the mandatory SIM Card registration was carried out to enable the use of surveillance equipment purchased and installed by telecom companies as per the law on the Interception of Communication Act, 2010.

How the right to privacy is being abused in Ugandan courts;

Despite the fact that every citizen has a right to privacy online free from surveillance, including the right to control how their personal data is collected, used, disclosed, retained and disposed; on a number of occasions courts have 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 with not 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.

Another case was; Criminal Case No. Criminal Case No. 0257 of 2010 Uganda Vs Akbar Hussein Godi In the matter of Mukono High Court before Justice Lawrence Gidudu. Prosecution evidence tendered phone printouts as expert evidence from Warid telecom and MTN to rebut Godi's alibi that sought to place him at the National Theatre in Kampala, and then his home on Entebbe road, places far from the murder scene in Mukono. The phone printouts showed that at the material time, Godi was, in fact, in Bweyogerere, along Jinja road, from where he called the deceased. The printouts also showed that the last communication between the couple took place at 7:30pm, just a few hours before the murder. The evidences tendered to court indicated that he also changed his phone number and stopped calling the deceased's sisters. Such conduct, the judge said, pointed to a guilty man.

In summary; while many Ugandans are not aware of the pending threats to the rights to privacy as government targets mobile phones used by most Uganda to seek to orchestrate illegal actions that aim at undertaking unprecedented surveillance of communications, little if any has been done to safe guard communication lines/ platforms to guarantee the freedoms of speech, expression, assembly and association online. The internet has provided expression platforms which otherwise would be closed like other traditional media expression outlets. The establishment of internet monitoring units among the various security agencies is cause of fear as it provides government agencies increased access to personal data especially taking advantage of the absence of established legislations that protect privacy and personal data in the hands of third parties.

This and much more point to the deteriorating trends among online activists and individual citizens who ordinarily use the internet as expression platforms.

SECTION 3: RECOMMENDATIONS AND CONCLUSIONS

Recommendations

a) To address the gaps in the regulatory bodies, there is need to enact the data protection, surveillance and privacy law and seriously implementing them, to ensure the right to privacy of different online users is guaranteed, and e-Government regulations through massive awareness creation and capacity building to support more online services and participation.

b) On the existing laws and policies, there is need to review some of these provisions such as the regulation of interception of communication Act, the Anti-terrorism Act among others, which infringe on personal privacy which should be amended or repeled to ensure that the right to privacy is guaranteed.

c) Set a standard security policy to enable organized approach through technical control in to the system such as fire walls.

d) There is need to develop and implement National Information Security Framework that will address issues of information security to create favorable online working environment for online service users

e) There is need to standardize certain security systems with international standards. Different countries have certain security standards, that are minimum standards for internet security, there is need for harmonizing such standards, say online banking

f) At organization and individual levels there need to customize platforms to make sure it suit the high end users. Sharing of pass words at organization level should be minimized.

g) Up dated technologies should be introduced at every level whether individual, organizational or national levels and there should be strict monitoring of the network.

h) To reduce online monitoring or surveillance it's recommended that activists add more security features on their sites such as https among others

i) All the internet users should be sensitized on this to keep secure information and build their legal knowledge capacities since one of the gaps is that the users even do not know the regulatory laws on internet security and do not observe the security guidelines.

j) Freedom of expression, speech, privacy and associations were identified by respondents as being violated and yet they are provided for and guaranteed in the Constitution. Some respondents recommended that to have smooth advocacy by HRDs, bloggers and others for common national interest, the state should respect the constitution and establish an enabling environment through which such freedoms of expression, speech, privacy and association on the internet shall be enjoyed by the citizens

k) Put measures in place that aim at implementing the UN resolution on protection of the right to privacy in the digital age

Conclusions

Freedom of the internet in Uganda like other freedoms enjoyed offline such as freedoms of speech, expression, opinion, thought and assembly and access to information are clearly facing distress and continuously becoming eroded notwithstanding that they are protected by various legal instruments. The internet provides the unrestricted platforms for expression and speech to millions of citizens. Through these platforms, citizens, netizens, individual human rights activists, anti-corruption activists, and journalists, risk arbitrary arrest, intimidation, threats and politically-motivated criminal charges for expressing views deemed by public authorities too critical or divergent which views are facing censorship in the mainstream traditional media.

Other than the internet, many of the expression platforms commonly used by activists have been closed down while others are being closely monitored. It is argued that the protection of the internet from surveillance and restriction will enhance the promotion, protection and respect of human rights especially activists' internet freedoms and digital rights. Like such rights ordinarily enjoyed offline, internet freedoms too need protection especially the freedoms of speech, thought, expression, association and assembly online.

REFERENCES

Daily monitor: Issue dated 30th December 2013

National Information Technology Authority – Uganda (2012) “Laws: Cyber Laws”, http://www.nita.go.ug/index.php/policies-and-laws/cyber-laws.

“Freedom House Condemns Crackdown on Journalists, Social Media in Uganda”, Freedom House, Press Release, April 22, 2011, http://freedomhouse.org/article/freedom-house-condemns-crackdown-journalists-social-media-Uganda.

The Parliament of Uganda (2013): Uganda Communications Commission.

Ekimeeza (2005): Global journalists

Whyte, A. and Macintosh, A. (2002): *‘Analysis and Evaluation of e-consultations’*; www.teledemocracy.org; accessed June 17

JOHN NASASIRA (2013), the Global e-Government Forum 2013

Freedom House (2013); Freedom on the Net, A global Assessment of Internet and Digital Media

KINTEX, Korea – 22nd – 23rd October, 2013

Unwanted Witness

Amplifying voices Changing lives

Plot 41 Gaddafi Road,
P.O.Box 71314 Clock Tower K'la
Tel: +256 414 697 635
Email: info@unwantedwitness.or.ug
Website: www.unwantedwitness.or.ug
Facebook: unwanted witness uganda
Twitter: @unwantedwitness