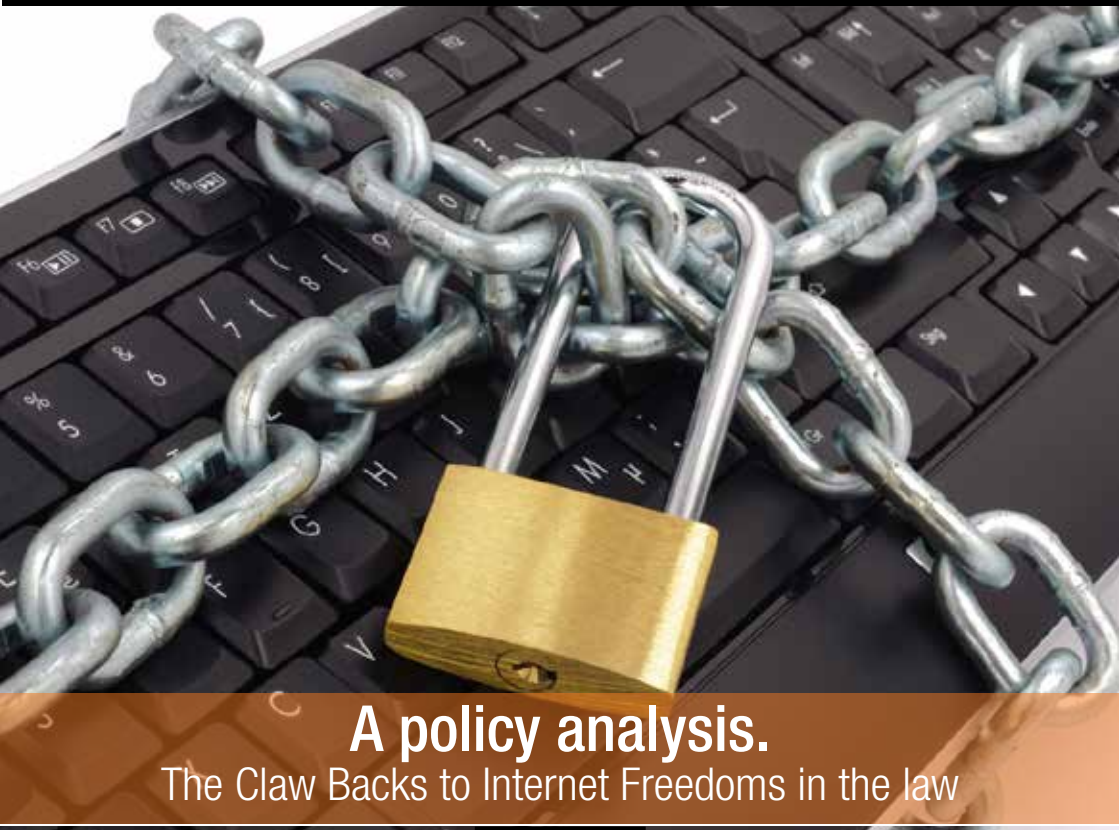
Unwanted Witness

Amplifying voices Changing lives

Digital Rights and Internet Freedoms in Uganda:



A policy analysis.

The Claw Backs to Internet Freedoms in the law

2015

Unwanted Witness

Digital Rights and Internet Freedoms in Uganda:

A policy analysis.

The Claw Backs to Internet Freedoms in the law

2015

TABLE OF CONTENTS

INTRODUCTION

The internet has increasingly become an integral part of everyday life for many people around the world. Together with other Information and Communication Technologies (ICTs), it has provided global citizens with an open platform to express themselves and as a result, improved the level of openness and public debate in the society[1].

Thanks to the Internet, traditional forms of communication – both print and broadcast – are no longer fully in charge of the information flow and no longer hold a monopoly over it. Anyone with access to a computer or a smartphone that is internet enabled can gather and disseminate information. Anyone can make their own broadcast. Anyone can publicly communicate their opinions and ideas to the entire world via a blog or social media network[2].

The internet has provided an alternative and escape from the challenges associated with the traditional media, especially the heavy censorship and harassment of journalists. The Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies[3]. A number of media outlets, journalists, citizens and bloggers have established blogs or social media platforms in order to reach a wider audience as well as exercise their right to freedom of expression.[4]

1 ARTICLE19 (2013) Freedom of Expression and ICTs: Overview of International standards
2 ARTICLE19 (2013) The Right to Blog; Policy Brief
3 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
4 Ibid

In Uganda, the internet has continued to proliferate, connecting more citizens to new digital media tools and platforms, particularly on internet-enabled mobile devices, in urban and rural areas alike.[5] According to the Uganda Communications Commission (2014), internet usage stands at 20 per cent while teledensity is only 52 cellphones per 100 inhabitants[6].

However, access and usability is still a challenge to many Ugandans. While the establishment of the National Optic Fibre Backbone is expected to enhance backbone connectivity to most of Uganda's borders, there is still a long way to go in enabling connectivity for the vast majority of Ugandans[7].

Additionally, the cost of access devices such as phones and computers is also still contributing to low levels of access to the Internet. Other barriers include the lack of appropriate local content and user-friendly applications that would have enhanced gainful use of Internet services. Other related challenges such as poor access and reliability of electricity supply as well as the lack of skills also persist[8].

But while there have been no reported incidents of government interference with the internet since April 2011[9], when the UCC issued a directive to internet service providers (ISPs) to temporarily block citizens' access to social media platforms during the national elections as well as during the "walk to work" protests[10] (over the rising cost of living); the threats to internet freedom in Uganda over the last few years have taken the form of legislative restrictions that significantly compromise peoples' right of access to information,

5 Freedom House (2014) Freedom on the Net in Uganda
6 UCC, Status of Uganda's Communications Sector, April 30, 2014
7 http://www.ucc.co.ug/data/edposts/12/Executive-Director%27s-International-Internet-Day-2014-message.html
8 http://www.ucc.co.ug/data/edposts/12/Executive-Director%27s-International-Internet-Day-2014-message.html
9 Freedom House (2014) Freedom on the Net in Uganda
10 CIPESA/ APC, (2012) Intermediary Liability in Uganda

freedom of expression including the media, and rights to privacy online[11] as provided for under the Access to Information Act 2005 and the 1995 Uganda Constitution, respectively.

Article 29 (1), Uganda's Constitution also provides for the right to freedom of expression including the media. The Constitution also provides for the right of Access to Information in the possession of the state or any other organ or agency of the state under Article 41.

But the right to freedom of expression goes hand in hand with the right to privacy, and this was recognised by the framers of the Uganda Constitution when they provided under Article 27 that; "no personal shall be subjected to unlawful search of the person, home or other property of that person or unlawful entry by others of the premises of that person. The article also provides that no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

Besides these domestic guarantors of the right to freedom of expression, is Uganda is a signatory to key International Covenants that provides for the rights to freedom of expression including online rights. These including, the Universal Declaration of Human Rights (Article 19), the International Convent on Civil and Political Rights (Article 19(2)) as well as the African Declaration on Human and Peoples' Rights (Article 9).

In his submission to the UN General Assembly, Frank La Rue[12], notes that by explicitly providing that everyone has the right to express him or herself through any media, Article 19 of the Universal Declaration of Human Rights and the ICCPR was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise

11 Ibid

12 UN Special Rapporteur on the Promotion and Protection of the right to Freedom of Opinion and Expression (August 2008 to August 2014)

their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet[13].

While freedom of expression and the right to privacy is not absolute, International law provides that these restrictions shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals (ICCPR 19(3).

Unfortunately, Uganda's legal adventures in the last few years has been anything but intended to protect and advance freedom of expression, both off and online and the right to privacy.

13 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

The Anti-Pornography Act, 2014[14]

In 2014, Uganda adopted the Anti-Pornography Act that criminalizes all forms of pornography.

The Act under Sections 13 & 14 creates 9 offences of which 4 rotate around production and distribution of pornographic materials. Specifically, S.3(1) states that; " A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography." On conviction, the offences attract a fine up to Uganda shillings ten (10) million (about USD 4,000) or imprisonment not exceeding 10 years or both (S.3(2)[15].

Section 14(1) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years of prison.

Section 17 of Act stipulates responsibility for the Internet Service Providers (ISPs) and makes them liable for content that is hosted or distributed on their platforms. Specifically, 17(1) states that any ISP who by not using or enforcing the means or procedure recommended by the Committee[16] to control pornography, permits to be uploaded or downloaded through its service any content of a pornographic nature, commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding five years or both.

14 http://www.ulii.org/content/anti-pornograpy-act-2014

15 Kimumwe P (2014) Media Regulation and Practice in Uganda: A Journalists' Handbook

16 Section 3 of the Act provides for a Pornographic Control Committee, whose functions as stipulated under Section 7(f) include advancing the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and television to detect and suppress pornographic material.

Additionally, Section 17 (2) makes it also possible for the court to for a subsequent offence to suspend the business of ISPs who commit an offence under subsection (1).

The Uganda Communications Act, 2013[17]

In 2013, the government passed the Uganda Communications Act 2013 to regulate the Ugandan communications services, as well as providing for the establishment of the Ugandan Communications Commission (UCC) (Section 4). Among its functions, the UCC is supposed to monitor, inspect, licence, supervise, control and regulate communications services; and (b), receive, investigate and arbitrate complaints relating to communications services and take necessary action (j) and establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators (u) and to set standards, monitor and enforce compliance relating to content (x) (Section 5).

While there had been some optimism with the enactment of this in terms of protecting peoples' right to privacy with sections 79 and 80, criminalising the infringement and punishment for unlawful interception and disclosure of private communication by a service provider – respectively, the same Act (section 5(u) has been used to establish the Social Media Monitoring Unit as well as the Interception of the Communications unit to conduct communication surveillance of individuals communication.[18] The effect of these types of actions on the Internet freedom of citizens with regard to both freedom of expression and privacy is obviously extremely hampering.

17 http://www.ucc.co.ug/files/downloads/UCC%20Act%202013.pdf

18 Witness -report "The Internet: They are coming for it too!", January 2014, https://www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf

The Anti-Terrorism Act, 2002[19]

The Anti-Terrorism Act includes provisions that provide for obtaining information in respect of acts of terrorism, which include the authorising of the interception of the correspondence of and the surveillance of persons suspected to be planning or to be involved in acts of terrorism. These provisions constitute a violation of right to privacy on the Internet, when digital communications are intercepted. The Act also includes provisions that threaten the freedom of expression.

Under Section 9(2), the Act provides that any person who, without establishing or running an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death.

What is exactly meant by promoting terrorism under Act is not well defined in the law so there is a risk of the provision getting a too wide and arbitrary scope of application. It is also difficult for media and individuals to know which type of material is seen as promoting terrorism. It can thus be thought that the requirements of unambiguous, predictable and transparent law are not fulfilled.

The Act also provides for the interception of communications and surveillance under part IIV. The Minister may designate an authorized officer who has the right to intercept the communications or a person and otherwise conduct surveillance in respect of a person or a group or category of persons suspected of committing any offence under Act.

19 http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf

Interception of e-mails and electronic surveillance fall under the scope of surveillance allowed under Act. The purposes for which interception or surveillance may be conducted are safeguarding the public interest, prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism, preventing or detecting the commission of any offence under Act and safeguarding the national economy from terrorism (Sections 18-19).

Obstructing authorized officer can result in a prison sentence of maximum two years (Section 20). None of these grounds is defined within the framework of the Act, which opens up for considerable abuse of the interception and surveillance powers as these can be based on loose and vague grounds. It is also in the power of the Minister to designate an authorized officer and there is no requirement of consideration from an impartial and independent judge of any kind. Even these provisions of ATA can thus be seen to contravene the principles of international human rights law.

The National Information Technology Authority, Uganda Act, 2009[20]

This law establishes the National Information Technology Authority in Uganda (NITA-U) as a government agency under the general supervision of the minister (Section 3 (3)). The objects of the NITA-U listed in Section 4 include diverse ways to promote information technology in Uganda and most of these aims are nothing but commendable. The functions of the NITA-U listed in Section 5 are many (18) and rather broadly formulated. Section 5 (18) extends the functions of the authority to undertake any other activity necessary for the implementation of the objects of the authority. The functions of the NITA-U that can be interpreted to constitute some level of threat with regard to freedom of expression and privacy are above all the following:

-to co-ordinate, supervise and monitor the utilisation of information

20 http://www.ulii.org/content/national-information-technology-authority-uganda-act-2009

technology in the public and private sectors (Section 5 (3)); this provision can be interpreted to threaten privacy and freedom of expression by allowing supervising and monitoring, whose scope is not clearly and unambiguously defined. It is not clear if by "utilisation" of information technology is understood access to Internet on more general level or a more content-specific use of Internet. The latter interpretation would open up considerable powers to supervise and monitor e.g. individuals' Internet traffic.

-to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals (Section 5 (4)); this provision opens up for the NITA-U to stipulate that public computers hardware or software that can restrict freedom of expression and privacy. It could for example be interpreted to allow for installation of filters, blocking mechanisms or spyware.

-to create and manage the national databank, its inputs and outputs (Section 5 (5)); the exact nature of the databank is not defined within the framework of the law and the unclear nature of data gathered in it can mean that personal data is processed in conflict with right to privacy.

-to set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organisation, sustenance, disposal, risk management, data protection, security and contingency planning (Section 5 (6)); this provision grants the NITA-U an extensive power to set standards with regard to different aspects of utilisation of information technology. Most of the issues can be seen to be related above all to the information technology infrastructure and access to Internet instead of actual content but above all the possibility to regulate data protection and security related to IT can open up for restrictions on the Internet content.

Part V of the NITA-U regulates the information technology surveys and powers of the authority. With information technology survey is understood an operation in which enumerations, inspections, studies, examinations, reviews, inquiries or analyses are carried out to collect or gather information

and data on matters related to information technology (Section 2). Section 19 (1) stipulates that the minister may, on the recommendation of the board direct, by a statutory order, that an information technology survey be taken by the authority on both public and private sectors. In carrying out such a survey the authority has power to collect information and data regarding information technology for the sector specified in the order and may use summons and search warrants to facilitate the enforcement of this collection of data and information (Section 19 (3) a-b). Section 20 (1) asserts further that where data or information on information technology is being collected in accordance with Section 19, the Executive Director, an officer of the Authority or an authorised officer, may require any person to supply him or her with any particulars as may be prescribed, or any particulars as the Executive Director may consider necessary or desirable in relation to the collection of the information. Furthermore, a person who is required to give information under subsection (1), shall, to the best of his or her knowledge and belief provide all the necessary information, in the manner and within the time specified by the Executive Director (Section 20(2)).

The powers of the authority are further expanded in Section 21, where it is stipulated that the staff of the Authority or an authorised officer may at all reasonable times enter and inspect any building or place and make such inquiries as may be necessary for the collection of information and data for a survey being carried out under Section 19. The right to enter a dwelling house is limited to the purposes of collecting information relating to information technology matters and for the exercise of functions under this Act.

The scope of different purposes for which information technology surveys can be conducted is not clearly defined. It is nevertheless expressly stated that they cover even the private sector. This combined with the long-going powers of entry and inspections means that it is difficult for individuals to foresee which types of information might be of interest for the NITA-U and can

thus end up as objects for inspection. This legislative framework can be seen to constitute a violation of privacy that is incompatible with the international human rights law as regards the requirement of predictable and transparent legal provisions. Section 22 stipulates that confidentiality is the main rule as regards for example data set or part of data stored in a computer or any other electronic media, but that does not affect the fact that NITA-U as a public authority has a possibility to get access to personal data about individuals.

What is another worrying aspect of the NITA-U is Section 34, where it is stated that The Minister may, after consultation with the Executive Director and the Board, give to the NITA-U directions of a general nature in writing, relating to policy matters in the exercise of the functions of the NITA-U and that it shall comply with any direction given by the Minister.

Section 39 further gives the Minister the power to, in consultation with the Board, by statutory instrument; make regulations generally for giving effect to the provisions of the act. These provisions can be seen to give a individual minister very wide powers, which also bring with itself a risk of misuse, as regards the functions of the authority.

The Regulation of Interception of Communications Act, 2010[21]

The Regulations of Interception of Communications Act (RICA) can be seen to be the most problematic law when it comes to guaranteeing the Internet freedom of Ugandan citizens. Section 3 of the Act provides for the establishment of a Monitoring Centre for the interception of communications under the Act. It is above all the minister responsible for security who is mainly responsible for establishing and running the centre.

21 http://www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

Under Section 4(1), an application for the lawful interception of any communication may be made by the Chief of Defence Forces, the Director General of the External Security Organisation, the Director General of the Internal Security Organisation, the Inspector General of Police or their nominees. A warrant to intercept communications shall be issued by a designated judge, by which is understood a judge designated by the Chief Justice to perform the functions of a designated judge for purposes of the Act (Section 1).

Section 5 lists the grounds on which the designated judge may issue a warrant to an authorized person. Although the interests that allow for issuing of a warrant can generally be seen as legitimate, the level of evidence the authorized persons are required to show is not higher than reasonable grounds for the designated judge to believe that a legitimate interest it at hand. It is thus very low level of evidence that is required so that a designated judge can issue a warrant under Act. This opens up naturally for abuse of both the power to apply for and to issue warrants. Neither are there any more specific requirements of impartiality, independence or competence stipulated when designating the responsible judge. The question is thus completely left to the discretion of the Chief Justice. When it comes to the actual grounds that make it legitimate to issue a warrant to intercept communications, it is the gathering information for any actual or potential threat concerning any national economic interest (Section 5 (c-d)) that is the most problematic provision.

Under Section 8, service provides are required to ensure that they are capable to enable the interception of communications. A failure to do this can result in a maximum prison sentence of five years. This provision threatens both privacy and freedom of expression on Internet as service providers, faced with the threat of criminal sanctions are forced to above all take to account the state's interests, not the individuals' interest to be able to enjoy their human rights.

Section 10 concerns notice on disclosure of protected information. By protected information is understood information that is encrypted by means of a key (Section 1). It is asserted in Section 10 that an authorized person may by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information, where he or she believes on reasonable grounds that that a key to any protected information is in the possession of any person, if he or she believes that the imposition of a disclosure requirement in respect of the protected information is necessary with regard to one of the interests and purposes that legitimate the issuing of warrants. Even here are present the low requirement of evidence, "reasonable grounds" while the "interest of economic well-being of Uganda" is listed as one of the grounds that give right to impose a disclosure requirement. It can thus be seen that the possibilities to impose an individual a requirement to disclose protected information are not protected by sufficient legal safeguards in the eyes of the international law. A person who fails to make the disclosure required by a notice can be liable to suffer a prison sentence of maximum five years (6). This penalty can be seen as disproportionate and combined with the loose grounds that enable requiring the disclosure can it be seen to contravene the international law.

Section 16 grants further the Minister power to by statutory instrument make regulations for carrying into effect the provisions of RICA. This can be seen to give one person a considerable amount of influence as regards the interception of communications. With this type of concentration of powers there is always a risk for abuse.

Amnesty International and the Special Rapporteur have also expressed their worries concerning several provisions of RICA. Amnesty has e.g. called for more precise definitions as regards the grounds for and the purposes of the interceptions of communications and surveillance. They also demand a clearer procedure as regards the appointment and operation of the designated

judge as well as independent oversight over both ministerial powers over the workings of the monitoring center and the actual operations of it. Amnesty also calls for an explicit provisions requiring judicial authorization for disclosure of protected information.[22] The Special Rapporteur has criticised the low threshold, which requires law enforcement authorities to only demonstrate that "reasonable" grounds exist to allow for the interception. According to the Special Rapporteur the burden of proof to establish the necessity for surveillance is extremely low given the potential for surveillance to result in investigation, discrimination or violations of human rights.[23]

The Electronic Signatures Act, 2011[24]

The Electronic Signatures Act 2011 regulates the use of electronic signatures in Uganda. There are some aspects of ESA that can be seen as creating risks as regards individuals' right to privacy and freedom of expression. ESA e.g. includes provisions on advanced electronic signature that are uniquely linked to signatory, reliably capable of identifying the signatory and linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable (Section 2). In case the security of these types of signatory systems is not adequate, the anonymity of a person's online behaviour can be threatened due to the possibility to identify the individual through his or her signature.
ESA also contains provisions concerning the public key infrastructure (PKI) that is controlled by the NITA-U, who is also responsible for licensing certification service provides (Part IV). NITA-U is responsible for monitoring and overseeing activities of certification service providers (Section 22). NITA-U further has far-reaching search powers as regards the activities of service provides. These include e.g. an unlimited access to computerised data (Section 88) and the

22 Amnesty International Memorandum on Regulation of Interception of Communications Act, 14 December 2010. See under "Conclusion" for a comprehensive list of recommendations by Amnesty International with regard to RICA.
23 SR, A/HRC/23/40, (56).
24 http://www.ulii.org/content/electronic-signatures-act

right to inspect, examine and copy computerised data kept by licensed certifications service provides (Section 91). The NITA-Us control over the public key infrastructure and long-going investigative powers combined with the fact that within the PKI are connected a certificate can be seen to open up for abuse as regards the anonymity and privacy of the individuals whose identities are connected to a certificate.

The Computer Misuse Act, 2011[25]

The Computer Misuse Act 2011 prescribes liability for offences related to computers. For example child pornography, cyber harassment, offensive communications, and cyber stalking are penalized under the Act. The maximum penalties for these offences range from one to five years of prison, with the exception of child pornography which can generate the maximum prison sentence of 15 years. The conditions required for these offences to be at hand are, however, often rather vaguely defined. This both contravenes the requirement of unambiguous and foreseeable provisions in international law and can have a hampering effect on freedom of expression.

The Act also penalizes unauthorized access to computer programs and data, unauthorized modification of computer material, unauthorized use of interception of computer service. The maximum penalties for these offences are between 10-15. Such heavy penalties can have a chilling effect on individual's use of computers in order to access to information and in order to use their freedom of expression. Section 18 further penalizes unauthorized disclosure of information with a maximum prison sentence of 15 years. It is stipulated that a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access. Such an vaguely formulated provision

25 http://www.nita.go.ug/sites/default/files/publications/Computer-Misuse-Act.pdf

restricting right to disseminate lawfully obtained information can seen to constitute a serious threat to freedom of expression online.

It is stipulated in Section 9 an investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification. This data includes traffic data and subscriber information. This provision can be seen to infringe on right to privacy, and indirectly even freedom of expression. Even though it is a court that decides over the preservation order, the grounds for issuing it are very vague. There is no requirement that an offence is suspected as it is enough that there are reasonable grounds to believe that the data is vulnerable to loss or modification. This provision can thus be seen to open up for abuse of the preservation orders and thus limit individuals' freedom on the Internet as it creates a risk for that e.g. information about their online traffic is preserved.

The investigative officer may also, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data or sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data (Section 10).

It is further stipulated that the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling any person to submit specified data in that person's possession or control, which is stored in a computer system and any service provider offering its services to submit subscriber information in relation to such services in that service provider's

possession or control (Section 11). The investigative officers have thus far-reaching powers to get access to information through a court order. It is not specified which type of offences make it possible for investigative officers to apply for a court order. The provisions can thus be interpreted to legitimate a court over even when the violation of privacy caused by the disclosure and submission of the data is not proportionate in relation to the seriousness of the offence. Apart from breaching privacy, these provisions can also indirectly have a chilling effect on freedom of expression when individuals are conscious of these possibilities for police to get access to their internet data.

Police officers have further long-going powers of search and seizure if they suspect that an offence under Act. It is asserted in Section 28 that where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing that an offence under Act has been or is about to be committed in any premises and that evidence that such an offence has been or is about to be committed is in those premises the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary. An authorised officer may seize any computer system or take any samples or copies of applications or data that are on reasonable grounds believed to be concerned or may afford evidence in the commission or suspected commission of an offence or are intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence. In order for these extensive search powers to be triggered the level of evidence required is low: the reasonable grounds for believing. These long-going powers of search and seizure combines with the low threshold of evidence required constitute a threat to privacy and freedom of expression. The police has broad powers to get access to people's computer data as thus violating privacy while the knowledge of these extensive powers can have chilling effect on the use of freedom of expression in the digital environment as people can be afraid of risking a police search on loose grounds.

The Electronic Transactions Act, 2011[26]

The Electronic Transactions Act provides for the use, security, facilitation and regulation of electronic communications and transactions. As regards possible threats to Internet freedom, the Act contains above all pertinent provisions concerning the liability of Internet service providers.
It is stipulated in Section 29 that a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on the making, publication, dissemination or distribution of the material or a statement made in the material or the infringement of any rights subsisting in or in relation to the material. This shall, however, not affect an obligation in contract, the obligation of a network service provider under a licensing or regulatory framework which is established by law or an obligation which is imposed by law or a court to remove, block or deny access to any material.

According to Section 30, a service provider is neither as liable for damage incurred by a user for referring or linking users to a data message containing an infringing data message or infringing activity if it does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user, is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent, does not receive a financial benefit directly attributable to the infringing activity removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user. Section 31 further prescribes that a person who complains that a data message or an activity relating to the data message is unlawful shall notify the service provider in writing and lists the particulars that such a complaint must contain.

26 http://www.ulii.org/content/electronic-transactions-act-2011

Although the service providers are consequently not as a main rule responsible for third party content, ETA makes it possible for Internet service providers to take down a data message if a person informs them that it is unlawful. There seems thus to be no requirement of court order in order for the service providers to be responsible to take down material that can be deemed unlawful. This can have a chilling effect on free speech as service providers can after a request from individuals to choose to take down material that an individual deems unlawful without the question being tried by a court.

It is further stated in Section 32 that service providers are not obliged to monitor the data which the service provider transmits or stores or actively seek for facts or circumstances indicating an unlawful activity. The Minister in consultation with the NITA-U may, however, by statutory instrument prescribe the procedure for service providers to inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service and communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority. It can be seen as problematic that minister and NITA-U have power to prescribe responsibilities for ISPs to inform the public authorities of illegal activities and help with the identification of Internet users.

There is no requirement that such statutory instruments would take necessary notice of the individual rights that can be infringed by imposing ISPs the responsibility to give authorities information and thus violate the privacy of individuals.

Recommendations

- The problematic provisions of the laws discussed above should be modified in order to become more transparent and unambiguous as regards the grounds on which freedom of expression and right to privacy can be limited in the digital environment.
- There should also be express guarantees as regards the need to assess the proportionality of the interference.
- The powers of the ministers as regards the infringements of rights should also be limited in favour of a system of independent and impartial judges.
- There is also a need to strengthen data protection. Thus it's recommended that a privacy and data protection law be enacted to give effect to Art.27 of the 1995 constitution, and the good news is that a draft Data Protection and Privacy Bill is now circulated for public consultation.[27]

27 The draft of the proposed bill can be found at http://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20PrivacyBill%20-%20Revised%20PDF.pdf

Plot 41 Gaddafi Road
P.O.Box 71314 Clock Tower K'la

Tel: +256 414 697 635
Email: info@unwantedwitness.or.ug
www.unwantedwitness.or.ug
Unwantedwitness-Uganda
@unwantedwitness
unwantedwitness