Analysed

CYBER LAWS

OF UGANDA

CIVIL RIGHTS DEFENDERS

WE EMPOWER PEOPLE

Unwanted Witness

Amplifying voices Changing lives

Analysed
CYBER LAWS
OF UGANDA

CIVIL RIGHTS DEFENDERS
WE EMPOWER PEOPLE

Unwanted Witness
Amplifying voices Changing lives

Published by:
Unwanted Witness

CITATION:
The Report can be cited as: 'Analyzed cyber laws of Uganda, 2016'

Design and Printed by:
Esam Concepts (U) Ltd, Tel: 0774438107

Table of Content

Acknowledgement

The Unwanted Witness (UW) and Civil Rights Defenders (CRD) jointly made the analysis published in this report.

The Analysis is only an assessment of Uganda's cyber laws from a human rights perspective that reflects on the compatibility of the provisions with Uganda's own 1995 Constitution and International Human Rights Standards. We hope this report will invite informed discussion and debates among policy makers and stakeholders to improve Uganda's respect for freedom of expression and online privacy and Digital rights.

We are indebted particularly to Anni Kolehmainen for her valuable contribution that culminated in this report.

Civil Rights Defenders further provided financial support for the publication of the report and advocacy project surrounding it. The Project is under implementation by Unwanted Witness in collaboration with the East & Horn of Africa Program at Civil Rights Defenders.

Unwanted Witness (UW) is a not for profit and non partisan registered civil society organisation working towards an open, free and secure Internet that contributes to the realization of human rights and good governance

Civil Rights Defenders (CRD) is an independent expert organisation founded in 1982 in Sweden, with the mission to defend people's civil and political rights and empower human rights defenders at risk worldwide. CRD has a presence on four continents and is active in some of the world's most repressive regions. By working in collaboration with 200 local partners and focusing on innovation, the goal is to achieve long-term sustainable change.

1 Background and the Aim of the Project

During the last decade several laws that have effect on the Internet freedom have been adopted in Uganda. The rights, which most significantly are threatened by these laws, are freedom of expression and the right to privacy. Some of these laws are pure cyber laws that take exclusively aim on the digital environment, whereas other laws are not exclusively directed on the digital environment but nevertheless contain provisions that have effect on the scope of online freedoms. Several provisions with potential to limit Internet freedoms of citizens can be identified among these laws. The relevant laws are the following:

3.1. The Anti-Terrorism Act, 2002
3.2. The National Information Technology Authority, Uganda Act, 2009
3.3. The Regulation of Interception of Communications Act, 2010
3.4. The Electronic Signatures Act, 2011
3.5. The Computer Misuse Act, 2011
3.6. The Electronic Transactions Act, 2011
3.7. The Uganda Communications Act, 2013
3.8. The Anti-Pornography Act, 2014

Currently, actions that threaten the enjoyment of online freedoms and rights in Uganda are stemming from the existing cyber legal framework.[1] The Ugandan cyber legislation gives government and its agencies unlimited powers with regard to procuring surveillance equipment[2] and criminalising gadgets (computers) as well as Internet content. Their powers range from illegally ordering Internet service providers to block certain social platforms[3] to signing secret memorandum of understanding among government agencies to share information about Internet users and published content in order to enforce the Ugandan cyber legislation.[4] Harassment of online activists by police has also been reported[5]

1 See http://www.refworld.org/pdfid/549026360.pdf for an overview over the state of Internet freedom of Uganda in 2014.
2 https://unwantedwitness.or.ug/the-unwanted-witness-uw-news-brief-state-house-is-procuring-surveillance-equipment/.
3 See e.g. http://www.reuters.com/article/2011/04/19/us-uganda-unrest-media-idUSTRE73I3LP20110419 and http://www.article19.org/data/files/pdfs/reports/world-press-freedom-day-no-frontiers-new-barriers.pdf.
4 https://unwantedwitness.or.ug/uganda-police-signs-a-secret-mou-with-uganda-communication-commission/.
5 https://unwantedwitness.or.ug/police-is-harassing-an-online-activist-in-mid-western-uganda/ and

These developments prove the urgent need to contiguously analyse the regulation of the Internet in order for citizens to be able to exercise fundamental freedoms, to be empowered and able to change their lives through the Internet. Many citizens view the Internet as one of the remaining independent platforms where a decent and sound debate can take place and where ideas can be shared without political interference. According to the Uganda Communication Commission the number of Internet users is growing steadily. The number of Internet users was estimated to be more than 8,5 million in June 2014.6

Against this background, surely analysing the Ugandan cyber legal framework from a human rights perspective is an important undertaking. The aim of this paper is to analyse the provisions of the laws that can be seen as restricting the Internet freedom of the citizens in Uganda. The principal purpose is to assess whether these provisions are compatible with international human rights standards on the freedom of expression and right to privacy. The second purpose is to support advocacy concerning Uganda's Internet freedoms.

The disposition of the analysis is the following: first the relevant international human rights standards regarding freedom of expression and right to privacy will be discussed (Chapter 2). Thereafter, relevant Ugandan cyber laws will be analysed in the light of international human rights law. The laws will be analysed in chronological order so that changes over time are made apparent (Chapter 3). This approach will also allow for a contextual understanding of the challenges that Uganda faces today regarding freedom on the Internet. In the final chapter the most important findings of the analysis will be discussed and summarized. Recommendations will be put forward as to how Ugandan cyber laws can be made better compatible with the international human rights standards on freedom of expression and right to privacy in the digital environment.

Securing access to the Internet for as many people as possible constitute an important part of Internet freedoms. The report will not deal with that particular question in detail. Instead it will focus on the analysis of legal restrictions that affect online freedoms of those who already have access to Internet.

Furthermore, the analysis will only focus on the provisions that are relevant to freedoms on the Internet. Other provisions that violate basic human rights but lack a direct connection to freedom on Internet are therefore not discussed in this report.

https://unwantedwitness.or.ug/police-extends-bond-for-the-online-activist/.
6 http://www.ucc.co.ug/data/qmenu/3/Facts-and-Figures.html.

2 The Guiding International Human Rights Standards

Provisions protecting freedom of expression and the right to privacy can be found in the majority of international human rights instruments. There are also international human rights standards that directly take aim at the protection of these rights in the digital environment. Not all of these standards are legally binding but can rather be seen as recommendations and soft law. Free speech and privacy guarantees in the international human rights instruments will be discussed in this chapter. Focus will primarily be on United Nations instruments of international scope. Thereafter relevant regional human rights instruments will be discussed. The legally non-binding recommendations and guidelines with regard to Internet freedoms will also be discussed.

As regards the protection of an individual's private life, a difference can be made between the right to privacy and data protection rights. It is also important to keep in mind that there is not one universally recognized definition of these rights. Although privacy and data protection overlap to a great extent, there is for example a specific provision for data protection in the EU Charter of Fundamental Rights alongside a provision protecting the respect for private and family life. Comprehensively defining "privacy" is a difficult, even close to an impossible, task. According to one definition, privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by

presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.

other uninvited individuals.[7] When it comes to data protection rights, in the Data Protection Directive of the EU (Directive 95/46/EC) personal data is defined to mean any information relating to an identified or identifiable natural person. One of the key differences between these two rights lies in that not all information relating to an identified or identifiable person need to fall within the scope of privacy. This makes the scope of data protection broader than the scope of privacy.[8]

2.1. The International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the General Assembly of the United Nations in 1966 and ratified by Uganda in 1995. The right to privacy is guaranteed in Art. 17 and freedom of expression in Art. 19. para. 2. It is stated in Art. 17 that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" (para. 1) and that "everyone has the right to the protection of the law against such interference or attacks." (para. 2). As regards freedom of expression, according to Art. 19 para. 2 "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

In the General Comment No. 34 to Art. 19[9] the Human Rights Committee (HRC), the body overseeing the implementation of the ICCPR, has asserted that it covers electronic and internet-based modes of expression.[10] It has also stated that states should take into account the extent to which developments in information and communications technologies, such as the Internet, have substantially changed the communications practices around the world.

7 SR A/HRC/23/40 (22).
8 See Kokott, J, & Sobotta, C, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, 2013, Vol. 3, No. 4, p. 225. This article provides an interesting and more comprehensive discussion on the topic on the European leve.
9 General Comment No. 34 to the Art. 19, Human Rights Committee, 102nd session, Geneva, 11-29 July 2011.
10 Ibid. (12).

This is due to there being a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. It is asserted that state parties should take all

necessary steps to foster the independence of these new media and to ensure access of individuals to them.[11] The free speech guarantees in ICCPR are thus applicable also on the Internet and states must guarantee the enjoyment of these rights in the digital environment.

In the same General Comment the HRC also stated that Art. 19 para. 2 includes the right to access to information held by public bodies. Such information includes records held by a public body, regardless of the form in which the information is stored, its source, and the date of production.12

All restrictions of freedom of expression must be provided by law and be necessary for; the respect of the rights or reputations of others, the protection of national security or public order (ordre public), or the protection of public health or morals (Art. 19 para. 3). The restrictions must also be proportionate.[13] The HRC has further emphasized that not under any circumstance, can an attack on a person, because of the exercise of his or her freedom of opinion or expression, be compatible with Art. 19. This includes arbitrary arrest, torture, threats to life and killing, [14]

The HRC has also asserted that a norm, in order to be characterized as a law, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. It must also be made accessible to the public. It is further affirmed that a law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Moreover, laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.[15]

11 Ibid. (15).
12 Ibid. (18)
13 Ibid. (34).
14 Ibid. (23).
15 Ibid. (25).

Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, must also be compatible with Art. 19 para. 3.[16]

Regarding counter-terrorism measures, the HRC has asserted that states parties should ensure that such measures are compatible with para. 3. This means that offences such as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. The HRC has also emphasized that excessive restrictions on access to information must be avoided. As media plays a crucial role in informing the public about acts of terrorism, its capacity to operate should not be unduly restricted and journalists should not be penalized for carrying out their legitimate activities.[17]

The General Comment No. 16 to Art. 17 was adopted in 1988, before the proper arrival of the digital era, and provides less up-to-date guidance as regards Internet freedoms than General Comment No. 34. It was, however, asserted already at that point in time that surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited under Art. 17.[18]

It was further stated that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Furthermore, effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process or use it and that it is never used for purposes incompatible with the ICCPR. Moreover, in order to have the most effective protection of one's private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes.

16 Ibid. (43).
17 Ibid. (46).
18 General Comment No. 16 to the Art. 17, Human Rights Committee, Thirty-second session, 8th of April 1988,(8).

Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control his or her files. If such files contain incorrect personal data or if data have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[19]

2.3. The Universal Declaration of Human Rights

The Universal Declaration of Human Rights (UDHR) was adopted by the General Assembly of the UN in 1948 and it contains guarantees for both right to privacy and freedom of expression.

The right to privacy is protected by Art. 12 of the Declaration, which states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Art. 19 provides guarantees for freedom of expression by asserting that everyone has the right to freedom of opinion and expression; including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

arbitrary interference with his privacy, family, home or correspondence,

2.4. Reports from the UN Special Rapporteur on Freedom of Expression

As regards freedom of expression, the UN human rights instruments are complemented by reports from the UN Special Rapporteur on Freedom of Expression (The Special Rapporteur).[20] The relationship between freedom of expression and Internet has been discussed by the Special Rapporteur in several reports. References to the relevant parts of the following reports will be made where appropriate during the later analysis:

19 Ibid. (10).

20 See http://www.ohchr.org/EN/ISSUES/FREEDOMOPINION/Pages/OpinionIndex.aspx for more information about the role of the Special Rapporteur.

-A/HRC/17/27, 16/05/2011, Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet.
-A/66/290, 10/08/2011, Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet.
-A/HRC/23/40, 17/04/2013, Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression.

2.5. The European Convention on Human Rights

The European Convention on Human Rights (ECHR) is the most important human rights instrument at the European level. It conforms to the standards set by the ICCPR. The right to respect for private and family life, home, and correspondence is guaranteed in Art. 8. Art. 10 provide protection for freedom of expression.

According to Art. 8 para. 1 everyone has the right to respect for his private and family life, his home and his correspondence. Art. 10 para. 1 states that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

These two rights may only be restricted in accordance with the law and each restriction must be necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Art. 8 para. 2); and in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary (Art. 10 para. 2). In order for the interference to be necessary in a democratic society, there must exist a pressing social need and it must be proportionate to the legitimate aim pursued.[21]

21 See e.g. CASE OF DUBSKÁ AND KREJZOVÁ v. THE CZECH REPUBLIC, 11/12/2014 and CASE OF GOUGH v. THE UNITED KINGDOM 28/10/2014 .

2.6. The EU Charter on Fundamental Rights

The EU Charter on Fundamental Rights (EUCFR) is the principal human rights instrument of the European Union.[22] It conforms in a great extent to the ICCPR and the ECHR but includes more far-reaching provisions on data protection than the other international human rights instruments. As regards the relationship between the EUCFR and ECHR, it is laid down in Art. 52(3) EUCFR that whenever the rights contained in the EUCFR correspond to those in the ECHR, the meaning and the scope of these rights will be the same. This does not, however, prevent the EU from providing more extensive protection for these rights. The accession of the EU to the ECHR has also been planned for a long time but remains yet to be completed.[23]

Art. 7 of the Charter provides protection for the right to respect for private and family life, home and communications. Art. 8 further guarantees protection for personal data concerning an individual. It is further stated in Art. 8 that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law and that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (para. 2). The compliance with these data protection rules shall also be subject to control by an independent authority (para. 3). In 2014 the European Court of Justice (ECJ) declared the EU:s Data Retention Directive (Directive No. 2006/24/EC) to be invalid as it entailed a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. According to the ECJ, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality.[24]

22 The EUCFR was first solemnly proclaimed by the Council of Ministers, the European Commission, and the European Parliament in 2000 and acquired full legal effect when the Lisbon Treaty came in force in 2009.

23 See e.g. Chalmers et al., European Union Law, 2014, p. 288 f. The draft agreement on the accession of the EU to the ECHR was reached in 2013 and has been critically commented by the Court of Justice of the European Union, see http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140180en.pdf.

24 The joined cases C-293/12 and C-594/12.

Freedom of expression is protected by Art. 11, which asserts that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (para. 1). It is further stated that the freedom and pluralism of the media shall be respected (para. 2).

It is further stated in Art. 52 that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2.7. The American Convention on Human Rights

The American Convention on Human Rights (ACHR) includes provisions protecting both right to privacy (Art. 11) and freedom of expression (Art. 13). Art. 11 stipulates that no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation and that everyone has the right to the protection of the law against such interference or attacks.

As regards freedom of expression, it is asserted in Art. 13 para. 1 that everyone has the right to freedom of thought and expression. This includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. This right shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure respect for the rights or reputations of others or the protection of national security, public order, or public health or morals (para. 2). Neither may the right of expression to be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions (para. 3).

2.8. The African Charter on Human and People's Rights

The African Charter on Human and People's Rights (ACHPR) is an inter-African human rights instrument which Uganda ratified in 1986. While there is no provision providing protection for the right to privacy, freedom of expression is protected by Art. 9 of the Charter. This includes right to receive information (para. 1) and right to express and disseminate opinions within law. This free speech provision can be seen to be more restrictive than the corresponding provisions in ICCPR, ECHR and ACHR as it stipulates a right to express and disseminate opinions within law without imposing any limitations on lawmakers as regards restricting freedom of expression in law.[25] Combined with the lack of the provision protecting the right to privacy, this makes the protection provided by the ACHPR for these two rights considerably weaker compared with the other international human rights instruments.

2.9. International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate)

The so called Necessary and Proportionate -principles are the result of a global consultation with civil society groups, industry, and international experts in Communications Surveillance law, policy, and technology. They attempt to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques. It is asserted that states must comply with each of the principles in order to actually meet their international human rights obligations in relation to Communications Surveillance. The principles in themselves are, however, not legally binding.[26]

25 Compare e.g. with Art. 11 in ACHPR protecting freedom of assembly where it is stated that "the exercise of this right shall be subject only to necessary restrictions provided for by law, in particular those enacted in the interest of national security, the safety, health, ethics and rights and freedoms of others."

26 https://en.necessaryandproportionate.org/text.

The fundamental principles of legality, legitimate aim, proportionality, necessity, as well as the principle of adequacy, are the starting point for Necessary and Proportionate- principles. Adequacy signifies that any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

When it comes to proportionality, it is stated that decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires states, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

1. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
2. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;
3. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;
4. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
5. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
6. information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
7. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

With competent judicial authority is understood an authority that is impartial and independent and 1. separate and independent 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, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation and safeguards against illegitimate access and right to effective remedy.

Other relevant principles included in the Necessary and Proportionate- principles are the requirements of due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation and safeguards against illegitimate access and right to effective remedy.

2.10. Joint Declaration on Freedom of Expression and the Internet

Joint Declaration on Freedom of Expression and the Internet declaration (JCFEI) was adopted in 2011 by the Special Rapporteurs for Freedom of Expression of the Americas, Europe, Africa, and the United Nations.[27] The four rapporteurs discussed the issues together with the assistance of ARTICLE 19, Global Campaign for Free Expression and the Centre for Law and Democracy.[28] JCFEI establishes guidelines in order to protect freedom of expression on the Internet.[29] The declaration is not legally binding but it specifies many of the principles found on the legally binding instruments as regards the enjoyment of freedom of expression online.

27 The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, Frank LaRue; the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) of the Organization of American States (OAS), Catalina Botero Marino; the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, Dunja Mijatoviæ; and the African Commission on Human and Peoples Rights (ACHPR) Special Rapporteur on Freedom of Expression, Faith Pansy Tlakula.

28 http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848.

29 Ibid.

The first of the principles states that freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards. These include the restrictions being provided for by law and necessary to protect an interest which is recognised under international law (the 'three-part' test)

(Art. 1 a). It is also asserted that when assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests (Art. 1 b).

Further, with regard to intermediary liability, it is stated that no one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle') (Art. 2 a). It is stated that at a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied) (Art. 2 b).

As regards filtering and blocking, it is laid down that mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse. (Art. 3 a). It is further stated that Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression (Art. 3 b).

2.11. The African Declaration on Internet Rights and Freedoms

The African Declaration on Internet Rights and Freedoms (ADIRF) is another document setting out principles that aim to strengthen freedom on the Internet.[30] Just like the Necessary and Proportionate - principles and JCFEI, it is not legally binding. It was launched in 2014 after more than twenty organisations having participated in the drafting process.

The development of the ADIRF is a Pan-African initiative to promote human rights standards and principles of openness in the Internet policy formulation and implementation on the continent. The intention with ADIRF is to elaborate on the principles which are necessary to uphold human and people's rights on the Internet, and to cultivate an Internet environment that can best meet Africa's social and economic development needs and goals.[31]

AIDRF provides protection for freedom of expression, right to information and right to privacy. It also states that the right to freedom of expression on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards (3 para. 2).

As regards freedom of information, it is asserted that all information, including scientific and social research, produced with the support of public funds should be freely available to all (4). With regard to freedom of expression, it is further stated that no one should be held liable for content on the Internet of which they are not the author and that state should not use or force intermediaries to undertake censorship on its behalf and intermediaries should not be required to prevent, hide or block content or disclose information about Internet users, or to remove access to user-generated content, including those that infringe copyright laws, unless they are required to do so by an order of a court.

30 africaninternetrights.org/declaration/.
31 http://africaninternetrights.org/about/.

What makes ADIRF particularly relevant in the African context is that it stipulates for protection of privacy and personal data as neither or these rights are included in the ACHPR. It is stated that everyone has the right to privacy online including the right to control how their personal data is collected, used, disclosed, retained and disposed of. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication (8 para. 1).

It is further affirmed, just as in case of freedom of expression, that the right to privacy on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards (8 para. 2). Collecting personal data is only allowed when it complies with well-established data protection principles. First, personal data or information must be processed fairly and lawfully; secondly, personal data or information must be obtained only for one or more specified and lawful purposes; thirdly, personal data or information must not be excessive in relation to the purpose or purposes for which they are processed; fourthly, personal data or information must be deleted when no longer necessary for the purposes for which they were collected.

When it comes to surveillance, it is stated that mass surveillance should be prohibited by law and that the collection, interception and retention of communications data amounts to an interference with the right to privacy whether or not those data are subsequently examined or used. It is also asserted that in order to meet the requirements of international human rights law, lawful surveillance of online communications must be governed by clear and transparent laws that, at a minimum, comply with the following basic principles:

-First, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime;

-Secondly, communications surveillance must be judicially authorized and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation.

-Thirdly, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

2.12. Summary

As the survey above has shown, both freedom of expression and right to privacy are universally protected in the majority of the international human rights instruments. Limiting these two rights requires as a rule that the restrictions are laid down in law and that a due notice is taken of the principles of necessity and proportionality. There is a broad consensus that freedom of expression and right to privacy should be guaranteed the same protection also in the digital environment. Besides the traditional free speech and privacy guarantees getting a new interpretation in the digital era, there are also several legally non-binding declarations that specifically take aim on guaranteeing these rights on the Internet.

3 The Ugandan Cyber Legislation

In this chapter Ugandan cyber law provisions will be analysed against the framework of international human rights law as described above. According to international law all restrictions of freedom of expression and right to privacy on the Internet must conform to the following three part test:

(a) Restrictions must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and

(b) Restrictions must pursue one of the purposes set out in Art. 19, para. 3 of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and

(c) Restrictions must be necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).[32]

The provisions analysed in the following are those, which can be seen to restrict the Internet freedom of Ugandan citizens by posing threats to freedom of expression and right to privacy in the digital environment.

In addition to the international human rights framework freedom of expression, freedom of information and right to privacy are also guaranteed in the Constitution of the Republic of Uganda, 1995. According to Art. 27 of the constitution, no person 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.

32 As summarised by the UN Special Rapporteur on Freedom of Expression (SR) in A/HRC/17/27 (24).

Furthermore, no person shall be subjected to interference with the privacy of his or her home, correspondence, communication or other property. Freedom of expression is protected by Art. 29 where it is stated that every person shall have the right to freedom of speech and expression, which shall include freedom of the press and other media. As regards freedom of information, it is stipulated by Art. 41 that every citizen has a right of access to information in the possession of the State or any other organ or agency of the State except where the release of the information can put the security or sovereignty of the State at risk, or interfere with the right to the privacy of any other person. It is therefore important to bear in mind that these rights are not only protected through international human rights instruments but also within the framework of the Ugandan constitution. Thus their continued derogation is contrary to Uganda`s international human rights commitments.

3.1. The Anti-Terrorism Act, 2002

The Anti-Terrorism Act (ATA) was adopted in 2002 and includes provisions that provide for obtaining information in respect of acts of terrorism. This includes the authorising of the interception of the correspondence and the surveillance of persons suspected to be planning or to be involved in acts of terrorism.

Section 9(1) states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism or training or mobilising any group of persons or recruiting persons for carrying out terrorism or mobilising funds for the purpose of terrorism commits an offence and shall be liable on conviction, to suffer death. It is further laid down in Section 9(2) of the ATA 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.

It is asserted by the UN Special Rapporteur that states are required under international law to prohibit incitement to terrorism in national criminal law, but such provisions must comply with the requirements of prescription by unambiguous law; pursuance of a legitimate purpose; and respect for the principles of necessity

and proportionality.[33] Furthermore, the Special Rapporteur has emphasized that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless it can be demonstrated that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.[34]

What is exactly meant by promoting terrorism under ATA is not defined in the law and there is hence 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 argued that the requirements under international law of unambiguous, predictable and transparent law are not fulfilled.

Publishing and disseminating material promoting terrorism can also result in an individual being convicted to the death penalty. According to the HRC, under no circumstances can an attack on a person, because of the exercise of his or her freedom of opinion or expression, including such forms of attack as arbitrary arrest, torture, threats to life and killing, be compatible with Art. 19. It is clear that disproportionate penalties on publishing and disseminating information of a type that is not clearly defined threatens the freedom of expression on Internet. That death penalty at all is applied in this context can in itself be seen as a serious infringement of the international human rights law.

Furthermore, the Special Rapporteur underlines that arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to that very right. This is due to it not only creating a "chilling effect", but also leading to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman or degrading treatment or punishment.[35]

33 SR, A/66/290 (81).
34 SR, A/HRC/17/27 (73).
35 Ibid. (28).

The interception of communications and surveillance within the framework of ATA is regulated in its part IIV. The responsible minister may designate an authorized officer who has the right to intercept communications and otherwise conduct surveillance in respect of a person or a group or category of persons suspected of committing any offence under ATA. Interception of e-mails and electronic surveillance fall under the scope of surveillance allowed according to ATA. 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 ATA and safeguarding the national economy from terrorism (Sections 18-19). Obstructing an authorized officer can result in a prison sentence of maximum two years (Section 20). None of these grounds is defined within the framework of ATA, which opens up for considerable abuse of the interception and surveillance powers as these can be based on loose and vague grounds. There is no requirement of authorisation, external control or review by an impartial and independent judge of any kind. Also these provisions of ATA can thus be seen to contravene the principles of international human rights law.

ATA has been criticised by Amnesty International in its report Stifling Dissent - Restrictions on the Rights of Freedom of Expression and Peaceful Assembly in Uganda.[36] The overly board definitions of "terrorism", "aiding and abetting" to terrorism and the fact that "promoting terrorism" is not defined under ATA are seen to be able to inhibit media work and criminalize legitimate media coverage. Even the interception powers of the authorized officers are criticised as they could make it possible to intercept communications between journalists and their sources.[37]

ATA consequently contains both provisions that constitute a violation of right to privacy on the Internet by providing for interception of digital communications and provisions that threaten the freedom of expression on the Internet.

36 Stifling Dissent - Restrictions on the Rights of Freedom of Expression and Peaceful Assembly in Uganda, Amnesty International, November 2011, https://www.amnesty.org/en/documents/AFR59/016/2011/en/.
37 Ibid., p. 14.

3.2. The National Information Technology Authority, Uganda Act, 2009

This law establishes the National Information Technology Authority in Uganda (NITA-U). It is a government agency under the general supervision of the minister responsible for information technology (Section 3 (3) and Section 2). The goals of the NITA-U listed in Section 4 include diverse ways to promote information technology in Uganda and most of these aims are 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.

Institutional Oversight and control of public servants
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:

Key Highlights On Specific Sections of NITA Act, 2009

(Section 5 (3); - to co-ordinate, supervise and monitor the utilisation of information technology in the public and private sectors

Analysis; this provision can be interpreted to threaten privacy and freedom of expression by allowing supervising and monitoring, the scope of which is not clearly and unambiguously defined. Moreover, it is unclear if by "utilisation" of information technology is understood access to Internet on a more general level or a more content-specific use of the Internet. The latter interpretation would open up considerable powers to supervise and monitor e.g. individuals' Internet traffic.

(Section 5 (4); - to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals

Analysis; this provision opens up for the NITA-U to stipulate standards for hardware and software in public computers that can restrict freedom of expression and privacy. It could for example be interpreted to allow for regulations requiring installation of filters, blocking mechanisms or spyware in public computers.

(Section 5 (5); - to create and manage the national databank,

Analysis; its inputs and outputs what is meant by the national databank is not defined within the framework of the law and it is neither made clear what type of data it consists of. Nor is it explained what is the origin of the data stored in the databank. It is thus unclear what type of data is collected in the national databank, who gathers the data, and who has the access to the data in the databank. This can mean both collecting and processing of personal data in a way that breaches the right to privacy. As the exact nature of the databank is not defined in the law and the character and origin of its data are unclear, there is a risk for personal data being processed in conflict with data protection principles. This could for example include collecting data based on individuals' behaviour on the Internet or making personal data digitally searchable in a way that infringes the right to privacy.

(Section 5 (6); - 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

Analysis; 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 the actual content. However, above all the possibility to regulate data protection and security related to information technology 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[38] direct, by a statutory order, that an information technology survey be taken by the authority on both public and private sectors. In

38 The Board of Directors appointed under Section 7 (Section 2). The Chairperson and the members of the Board are appointed by the Minister, with the approval of Cabinet (Section 7 (2).

carrying out such a survey the authority has the power to collect information and data regarding information technology for the sector specified in the order. It may use summons and search warrants to facilitate the enforcement of such collections of data and information (Section 19 (3) a-b).

Section 20 (1) stipulates 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.

It is further laid down in Section 38(4) that a person who for example hinders or obstructs the Executive Director, an officer of the Authority or an authorised officer in the lawful performance of any duties or in lawful exercise of any power imposed or conferred on him or her under NITA-U commits an offence. The same goes for a person who for example refuses or neglects to complete and supply, within the time specified for the purpose, the particulars required by the Authority in any return, form or other document, to answer any question or inquiries put to or made of him or her, under this Act. A person who commits such an offence is liable, on conviction, to a fine not exceeding twelve currency points or imprisonment not exceeding six months, or both.

Analysis; The scope of different purposes for which information technology surveys can be conducted is not clearly defined. It is however, expressly stated that they cover both the public and private sector. This combined with the far-reaching powers of entry and inspections means that it is difficult for individuals to foresee what kind 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. However, this does not affect the fact that the NITA-U as a public authority has a possibility to get access to personal data concerning individuals.

According to Section 34, the Minister may, after consultation with the Executive Director and the Board, give NITA-U directions of a general nature. Such directions shall be in writing and relate to policy matters in the exercise of the functions of NITA-U. NITA-U shall comply with any direction given by the Minister. The particulars of any directions given by the Minister shall be included in the annual report of the Authority, together with the extent to which the directions were complied with. It is stipulated in Section 36 that The Board shall cause to be prepared and shall submit to the Minister within three months after the end of each financial year, an annual report on the activities and operations of the Authority for that financial year. According to Section 37 The Minister shall in each financial year, submit to Parliament as soon as possible after receiving them, the Auditor General's report and the annual report of the Authority. This can be seen as the only means of external control in relation the Minister's actions in relation to the NITA-U. Section 39 gives the Minister the power to, in consultation with the Board, make regulations generally for giving effect to the provisions of the act by statutory instrument. These regulations may prescribe, in contravention with the regulations, a prison sentence up to two years; three years in case of second of subsequent offence.

Analysis; These provisions can be seen to give the responsible minister wide powers, which also bring with itself a risk of misuse, as regards the functions of the authority.

Although there is a certain parliamentary control involved in the form of annual report, the Minister still has possibility to for example stipulate offences resulting in prison sentence.

3.3. The Regulation of Interception of Communications Act, 2010

The Regulations of Interception of Communications Act (RICA) is probably the most problematic law when it comes to guaranteeing the Internet freedom of Ugandan citizens. Section 3 of RICA provides for the establishment of a Monitoring Centre for the interception of communications under the act. The minister responsible for security is mainly responsible for establishing and running the centre.
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 (Section 4 (1)), also referred to as authorized persons (Section 1). 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 RICA (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 a very low level of evidence that is required for a designated judge to be able issue a warrant under RICA. This naturally opens up 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 decision 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. What is meant by a national economic interest is not defined within the framework of RICA and it can thus be loosely interpreted to mean many different things. It can therefore be seen

to conflict with the requirement of transparency and unambiguous legislation in international human rights law. Combined with the low requirement of evidence and the lack of requirements of objectivity and impartiality with regard to the designated judge, this point can above all render possible the abuse of the power to intercept communications. The lack of requirement of objectivity and impartiality as regards the designated judges can above all constitute a threat by making judges economically corruptible.

When it comes to service providers, they are required under Section 8 to ensure that they have installed relevant equipment with capability to enable the interception of communications. A failure to do this can result in a prison sentence up to five years. This can be seen to threaten both privacy and freedom of expression on the Internet as service providers are with the threat of criminal sanctions forced to take into account the state's interests, not the individuals' interest to be able to enjoy their human rights. The balancing of interests made my legislator is thus clearly tipped in favour of the national interests instead of the individual rights. Combined with the vague grounds for interception and the discretion of the judges, can this balance of interests on the whole be seen to constitute a disproportionate infringement of an individual's privacy.

Telecommunications service providers also have a duty to ensure that subscribers register their SIM-cards and provide service provides with comprehensive information about e.g. their identity and address (Section 9). This requirement of SIM-card registration can be seen to gravely undermine the Internet freedom of those who choose to use their mobile phones to surf on the web, as it is possible to directly connect their online activities to their identities. There are consequently provisions requiring service providers to enable the interception of communications in the state's interest while provision protecting the privacy and personal data of the affected individuals are considerably weaker. On top of these concerns, service providers (telecom companies) have embedded terms and conditions on the SIM card registration forms that can endanger people's privacy. These include handing over people's collected data to government upon request with or without the owner's permission or consent. There are also concerns by service providers making disclaimers at registration of SIM cards to be able to provide user identification to authorities when requested.

Section 10 concerns notice on disclosure of protected information. By protected information is understood information that is encrypted by means of a key as per Section 1 of the Act. 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. This can be done when the authorized person believes on reasonable grounds that a key to any protected information is in the possession of any person. It is also possible to impose a disclosure requirement if the authorized person 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. Again, the low requirement of evidence "reasonable grounds" appears, and the "interest of economic well-being of Uganda" is listed as one of the grounds that give right to impose a disclosure requirement. Thus, the possibilities to impose on an individual a requirement to disclose protected information are not combined with sufficient legal safeguards as required under international law. A person who fails to make the disclosure required by a notice can be sentenced to a prison sentence of up to five years (Section 10 (6)). This penalty can be seen as disproportionate and, combined with the loose grounds that enable requiring the disclosure, to contravene the international law.

Amnesty International and the Special Rapporteur have also expressed their worries concerning several provisions of RICA. Amnesty called for more precise definitions regarding 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 centre and the actual operations of it. Amnesty also calls for an explicit provisions requiring judicial authorization for disclosure of protected information.[39] 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.

39 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.

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.[40]

3.4. The Electronic Signatures Act, 2011

The Electronic Signatures Act (ESA) regulates the use of electronic signatures in Uganda. While promoting the use of electronic signatures can generally be regarded as a positive development, there are some aspects of ESA that can be seen as creating risks in relation to individuals' right to privacy and freedom of expression. ESA for example 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 are also responsible for licensing certification service provides (Part IV). The 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 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 far-reaching investigative powers combined with the fact that individuals' identities within the PKI are connected to 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.

40 SR, A/HRC/23/40, (56).

3.5. The Computer Misuse Act, 2011

The Computer Misuse Act (CMA) prescribes liability for offences related to computers. For example child pornography, cyber harassment, offensive communications, and cyber stalking are penalized under CMA. 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.

CMA 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 years. 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 a vaguely formulated provision restricting the right to disseminate lawfully obtained information can constitute a serious threat to freedom of expression online.

It is stipulated in Section 9 that 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 the right to privacy, and indirectly on the freedom of expression. Even though it is a court that decides over the preservation order, the grounds for issuing it are very vague. According to Section 9 (3) the preservation order shall remain in force until such time as may reasonable be required for the investigation of an offence or, where prosecution is instituted, until the final

determination of the case until such time as the court deems fit. There is, however, no express requirements as to the level of evidence required when applying for a preservation order. It is enough that there are reasonable grounds to believe that the data is vulnerable to loss or modification, while nothing is said as regards any suspected offence. This can lead to preservation orders being issued without the level suspicion being proportionate to the infringement of privacy the preservation of computer data can result in. 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 that e.g. information about their online traffic is preserved. It is not defined in the provision who can be targeted by a preservation order. It can thus be interpreted to impose the responsibility to preserve data to service providers as well as private individuals.

The investigative officer may also, for the purpose of a criminal investigation or the prosecution of an offence, apply to a court of law 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 where 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. It is neither specified which level of suspicion is required for a court order to be issued. The provisions can thus be interpreted to open up for issuing a court order 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. In the same way, a court order could be issued when the level of suspicion is not strong enough to render the disclosure of data proportionate as regards the ensuing violation of privacy. These provisions can consequently be seen to lack adequate privacy guarantees when it

comes to the rights of authorities to access computer data, either through service providers or private individuals. Apart from breaching privacy, these provisions can also indirectly have a chilling effect on freedom of expression as it is possible for authorities to get access to individuals' Internet communications on unclear and unforeseeable grounds.

Police officers further have far-reaching powers of search and seizure if they suspect an offence under CMA. It is asserted in Section 28 that where a Magistrate is satisfied by information given by the police that there are reasonable grounds for believing that an offence under CMA 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 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: only amounting to the reasonable grounds.

These far-reaching powers of search and seizure combined with the low threshold of evidence required constitute a threat to privacy and freedom of expression. The police have broad powers to get access to people's computer data, which creates risk for violating privacy. In addition, the awareness 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.

3.6. The Electronic Transactions Act, 2011

The Electronic Transactions Act (ETA) provides for the use, security, facilitation and regulation of electronic communications and transactions. As regards possible threats to Internet freedom, ETA 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 a contractual obligation, 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 not 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; or

- 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.

Although the service providers are 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 a minister and the NITA-U have the power to prescribe responsibilities for Internet service providers 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 Internet service providers the responsibility to give authorities information and thus violate the privacy of individuals.

3.7. The Uganda Communications Act, 2013

The Uganda Communications Act (UCA) regulates the Ugandan communications services. It provides for the establishment of the Ugandan Communications Commission (UCC) (Section 4). Functions of the UCC include e.g. to monitor, inspect, licence, supervise, control and regulate communications services (b), to 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). The UCC shall exercise its functions independently (Section. 8) while the Minister may, in writing, give policy guidelines to the Commission regarding the performance of its functions and it shall comply with these guidelines (Section 7).

The functions of the UCC open up for extensive possibilities to supervise and control the communications falling under the scope of UCA. This also makes it possible for it to act in a way that infringes both privacy and freedom of expression. Section 5(u) has for example been used to establish the Social Media monitoring centre and the interception of Communication monitoring centre under RICA to conduct

communication surveillance of individuals' communications for example on the Internet.[41] Government has also recently threatened to completely block the usage of social media platforms such as Facebook and WhatsApp.[42] 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.

3.8. The Anti-Pornography Act, 2014

The Anti-Pornography Act (APA) was adopted in 2014 and criminalizes all forms of pornography. According to Section 13(1), a person shall not produce, traffic in, broadcast, procure, import, export, sell or abet any form of pornography. An offence under this paragraph can result in a prison sentence of maximum ten years (Section 13 (2)). Section 14(1) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years. The realization of APA is overseen by the Pornography Control Committee established in Part II.

Pornography is defined within the framework of APA to mean any presentation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or stimulated explicit sexual activities or any representation of the sexual parts of the person primarily for sexual excitement.

APA consequently prohibits all forms of pornography and covers also pornographic presentations through information technology. An all-out prohibition of pornography can in several cases be seen to restrict freedom of expression in the digital environment. The definition of pornography is not exact enough to enable media and individuals to know for certain which presentations fall within the scope of APA. According to the Special Rapporteur, the only form of pornography that the states are allowed to prohibit is child pornography.[43] States are even required

41 Unwanted 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.
42 https://unwantedwitness.or.ug/uw-news-brief-ucc-threatens-to-shut-down-social-media-platforms/.
43 SR, A/HRC/17/27, (25), (32).

to do so under international law.[44] In Ugandan law the sentences in cases of both pornography and child pornography are very heavy. As mentioned above, arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to freedom of expression. Prohibition of all forms of pornography can accordingly be seen to both limit the right to freedom of expression on the Internet and contravene the international human rights standards.

Moreover, the right to privacy is threatened within the framework of APA. Section 24 stipulates that a register of pornography offenders containing the name of every person convicted of an offence under APA shall be maintained. The creation of this type of register can be seen to contravene both the privacy standards in international human rights law and the data protection principles.

It is laid down in Section 15 (1) that where information is brought to the attention of court that there exists in premises, an object or material containing pornography or an act of event of a pornographic nature, the court shall issue a warrant for the seizure of the object or material and for the arrest of the person promoting the material or object. An authorized person[45] in possession of a search warrant issued by the court may enter any premises and inspect any object or material including any computer, and seize the object, material or gadget for the purpose of giving effect to APA (2). Consequently, if someone makes it known to the court that someone is in possession of pornographic material, the court shall issue a warrant that makes it possible to enter the suspect's home and inspect and size the individual's computer. The level of evidence required for the court to issue a warrant is not specified more closely, which means that the provision can make it possible for authorized officers to get access to an individual's computers without there being any real evidence of the existence of pornographic material. It is also asserted in Section 24 (3) that anyone who obstructs an authorized officers commits and offence and can suffer the maximum sentence of five years. With regard to the fact that the universal criminalization of pornography can be seen to contravene international human rights principles and that the definition of pornography is vague, Section 15 can be seen to constitute a disproportionate violation of privacy.

44 SR, A/66/290, (18), (81).
45 According to Art. 1, by "authorized person" is understood a member of the Pornography Control Committee or a police officer.

Section 17 of APA also stipulates responsibility for Internet service providers. It is laid down that an Internet service provider who, by not using or enforcing the means recommended by the Committee to control pornography, permits to be uploaded or downloaded through its service any content of pornographic nature, commits an offence which can result in a prison sentence of maximum of five years (1). Section 17 (2) also makes it possible for the court to for a subsequent offence to suspend the business of Internet service providers who commit an offence under (1). In JDFEI it is emphasized that no one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so. Within the framework of APA the individuals behind Internet service providers risk a prison sentence of maximum five years for allowing individuals to upload and download pornographic material. It is also the Committees recommendations, not a court order, which lay as the basis for the Internet service providers' obligations. Such a long-going intermediary liability that is not based on a court order and has as an aim to prevent in many case legitimate expression cannot be considered to be compatible with international human rights standards.

4 Summary and Recommendations

The Ugandan cyber laws analysed above contain many deficiencies as regards their compatibility with international human rights standards. Criminalization of certain forms of expression (e.g. the all curtailment of access to social media under the pretext of national security as witnessed during the 2016 general elections), can in itself be seen to contravene international human rights law. At the same time the more legitimate criminalization of certain forms of expression (terrorism, child pornography) is based on vague, loose definitions, formulations and can result in disproportionate penalties.

The right to privacy is threatened under the Ugandan cyber laws as various provisions enable both targeted and mass surveillance of individuals' communications, as well as search and seizure of private mobile electronic gadgets and computers. This position is not only legitimized under the RICA, as has been analysed above, but also several of the other analysed laws contain provisions which make it possible to intercept individual's communications and search private property. The level of evidence required for a warrant to be issued is as a rule extremely low and the judicial involvement in the process of issuing warrants is either unclearly defined or lacking totally. independent oversight is both lacking in want and has no technical capacity. The laws lack more long-going guarantees for the protection of the right to privacy and protection of personal data in the wake of recent revelations by civil society groups under the Funga Macho report.[46]

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. Interventions that seek to strengthen adherence to the rule of law by both individual officers and especially security institutions should be prioritized.

46 https://www.privacyinternational.org/node/656

There should also be express guarantees as regards the need to assess the proportionality of the interference. This should take into consideration repealing or making necessary amendments to such laws that affect the full enjoyment of the rights and freedoms discussed above. Specifically the government should consider enacting the Privacy and Data Protection Law that has been shelved since 2014 to guarantee the full realization of the right to privacy in the wake of continued targeted surveillance by security agencies.

Establish independent oversight bodies and procedures over such actions that have the capability of negatively impacting fundamental rights and freedoms. The powers of the ministers as regards the infringements of rights should also be limited in favor of a system of independent and impartial judges or oversight commissions.

Related to the above, there is also a need to strengthen data protection. The long overdue privacy and data protection law should be enacted to give effect to Art. 27 of the 1995 Constitution. The mass enrollment exercise, together with the compulsory SIM card registration are likely to expose many citizens data to third parties in the absence of data protection mechanisms.[47]

47 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