Unwanted Witness

Amplifying voices Changing lives

REPRESSIVE:

UGANDA'S WORST CYBER LAWS THREATENING FREE EXPRESSION AND PRIVACY.

REPRESSIVE:

UGANDA'S WORST CYBER LAWS THREATENING FREE EXPRESSION AND PRIVACY.

BACKGROUND

The last decade, the Ugandan government has enacted eight (8) pieces of legislations that have serous effects on the enjoyment of Internet freedom namely; the Anti-Terrorism Act, 2002; the National Information Technology Authority, Uganda Act, 2009; the Regulation of Interception of Communications Act, 2010; the Electronic Signatures Act, 2011; The Computer Misuse Act, 2011; the Electronic Transactions Act, 2011; the Uganda Communications Act, 2013 and the Anti-Pornography Act, 2014. In 2015, the Unwanted Witness undertook an exercise to understand general effects the above outlined laws have on enjoyment of digital rights and freedoms as enshrined in the 1995 Constitution of the Republic of Uganda and International human rights laws to which, Uganda has assented to.

Regarding this study, the Unwanted Witness and partners including Internews agreed to identify, take a deeper scrutiny of the most repressive cyber laws. After the process of scrutinizing, three (3) out of the eight cyber laws on the land namely; Anti-Pornography Act, 2014, Regulation of Interception of Communications Act, 2010 and the Anti-Terrorism Act, 2002 were ranked as the worst and threatening the enjoyment of digital freedoms.

Uganda is party to several international agreements that protect freedom of expression and the right to privacy, including the African Charter on Human and Peoples' Rights and the International Covenant on Civil and Political Rights. As a State Party, Uganda has an obligation to implement and act in accordance with these treaties,[1] which includes an obligation to protect freedom of expression and privacy online. Uganda's Constitution protects freedom of expression in Article 29(1)(a) and the right to privacy in Article 27.[2]

Section I of this document sets out Uganda's obligations under international law regarding the right to freedom of expression and the right to privacy. Section II assesses the compliance of the Regulation of Interception of Communications Act, the Anti-Terrorism Act, and the Anti-Pornography Act with these standards, making recommendations for their improvement.

1 Vienna Convention on the Law of Treaties, 23 May 1969, UN Doc. A/Conf.39/27, Articles 18 and 31; African (Banjul) Charter on Human and Peoples' Rights, 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, Article 1; International Covenant on Civil and Political Rights, 16 December 1966, UN Doc. A/6316, Article 2.

2 Constitution of the Republic of Uganda, 22 September 1995.

I. INTERNATIONAL STANDARDS THAT PROTECT THE RIGHT TO FREEDOM OF EXPRESSION AND PRIVACY

A. Treaties

International Covenant on Civil and Political Rights

Uganda ratified the International Covenant on Civil and Political Rights ("ICCPR")[3] in 1995.[4] Consequently, all organs of the Ugandan State are obligated to implement and act in accordance with its treaty provisions.[5]

The ICCPR affirms the right to freedom of expression in Article 19, which states that "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."[6]

The right to freedom of expression is not absolute and can be restricted under limited circumstances. The conditions for legitimate restrictions are set out in ICCPR Article 19(3). In order to be permissible under international law, a restriction to the right to freedom of expression must be:

- Provided by law;
- Imposed in pursuit of a legitimate aim, namely the rights or reputations of others, the protection of national security, public order, or public health or morals; and
- Necessary and proportionate.[7]

Restrictions on the right to freedom of expression are only permitted when all parts of this three-part test are met.

3 International Covenant on Civil and Political Rights, supra note 1.
4 See Office of the High Commissioner for Human Rights website: http://indicators.ohchr.org/.
5 Vienna Convention on the Law of Treaties, supra note 1, Articles 18 and 31.
6 International Covenant on Civil and Political Rights, supra note 1, Article 19.
7 Id.

For a restriction to be characterised as "provided by law", it must be made accessible to the public and formulated with sufficient precision to enable individuals to regulate their conduct accordingly.[8] The restriction also needs to provide sufficient guidance to those charged with its execution to enable them to determine what type of expression is restricted and what is not. Importantly, the UN Human Rights Committee ("UNHRC") has stated that "A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[9]

Freedom of expression can be permissibly restricted only for one of the legitimate aims listed in ICCPR Article 19(3). Restrictions on grounds other than the rights or reputations of others, the protection of national security, public order, or public health or morals are therefore never in accordance with international law.

To meet the requirement of necessity and proportionality, the restriction must be necessary to achieve a legitimate purpose and not be overbroad. The UNHRC specified this as follows:

> *"restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law."*[10]

The UNHRC has affirmed that the right to freedom of expression covers electronic and internet-based modes of expression.[11]

ICCPR Article 17 affirms the right to privacy: "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" and "Everyone has the right to the

8 UNHRC, General comment No. 34, Article 19: Freedoms of opinion and expression ("General Comment 34"), 12 September 2011, CCPR/C/GC/34, par. 25.
9 8 General Comment 34, supra note 8, par. 25.
10 UNHRC, General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9, par. 14. See also General Comment 34, supra note 8, par 34.
11 General Comment 34, *supra* note 8, par. 12.

protection of the law against such interference or attacks."[12] The requirement that an interference with the right to privacy must be lawful and non-arbitrary means that the test for permissible restrictions on privacy is essentially the same as for freedom of expression.[13]

The right to freedom of expression and privacy are intertwined: without adequate protection of the right to privacy, the right to freedom of expression is also harmed. The UN Special Rapporteur on the right to freedom of opinion and expression ("UN Special Rapporteur") put it as follows:

> *"States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny. In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks." 14*

12 International Covenant on Civil and Political Rights, supra note 1, Article 17.

13 See UNHRC, ICCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. See also UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4;
Peoples' Rights, UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 1999, A/HRC/13/37.

14 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, A/HRC/23/40, par. 79-80.

African Charter on Human and Peoples' Rights

Uganda ratified the African Charter on Human and Peoples' Rights ("African Charter") in 1986.[15] While there is no provision protecting the right to privacy, the right to freedom of expression is protected by Article 9 of the Charter. This includes the right to receive information and right to express and disseminate opinions within the law.[16] The African Charter stipulates in Article 27 that this right shall be exercised "with due regard to the rights of others, collective security, morality and common interest."[17] While Article 9 does not place any limitations on the legal restriction of freedom of expression, the African Commission on Human Rights and Peoples' Rights ("African Commission") has stated that "[a]ny restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary in a democratic society."[18] Therefore, the ICCPR three-part test also applies under the African Charter. The African Court on Human and Peoples' Rights ("African Court"), the only body that can make binding decisions on violations of the African Charter, has indeed applied the three-part test in its freedom of expression jurisprudence.[19]

East African Community Treaty

Uganda is a member of the East African Community. The Community's constitutive document, the East African Community Treaty (the "Treaty"), lays out democracy, the rule of law, and human and peoples' rights as its fundamental and operational principles.[20] The East African Court of Justice in Burundi Journalists Union v.

15 African Commission on Human and Peoples' Rights, ratification table: http://www.achpr.org/instruments/achpr/ratification/.
, Article 27. Available at: fication status of human rights treaties by Uganda "Every individual shall have the right to receive information … Every individual shall have the right to express and disseminate his opinions within the law." African Charter on Human and Peoples' Rights, supra note 1, Article 9.

16 African Charter, supra note 1, Article 27.

17 African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression in Africa, 22 October 2002.

18 See African Court on Human and Peoples' Rights, Lohé Issa Konaté v. Burkina Faso, Application No. 004/2013, 5 December 2014.

19 East African Community, Treaty for the Establishment of the East African Community, 30 November 1999, Articles 6 and 7.

20 East African Court of Justice, Burundi Journalists Union v. The Attorney General of the Republic of Burundi, Reference No. 7 of 2013, 15 May 2015.

The Attorney General of the Republic of Burundi[21] held that it had jurisdiction to consider claims concerning a violation of the right to freedom of expression under Articles 6 and 7 of the Treaty.[22] As a member of the East African Community, Uganda is subject to the East African Court of Justice's jurisdiction regarding its compliance with the Treaty in protecting the right to freedom of expression.

B. Non-binding international standards

While non-binding, the following declarations, resolutions and agreements are relevant normative standards to further interpret Uganda's obligations under international law regarding freedom of expression and the right to privacy.

Universal Declaration of Human Rights

The Universal Declaration of Human Rights ("UDHR")[23] provides for freedom of expression and the right to privacy under Articles 19 and 12, respectively. Article 19 states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Article 12 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."[24] While the UDHR is not a legally binding treaty, it is a fundamental constitutive document of the United Nations and an important normative standard of international law.

21 Article 6 states that the fundamental principles of the Community shall include "the recognition, promotion and protection of human and peoples rights in accordance with the provisions of the African Charter on Human and Peoples' Rights" and Article 7 states that "The Partner States undertake to abide by the principles of good governance, including adherence to the principles of democracy, the rule of law, social justice and the maintenance of universally accepted standards of human rights."

22 Universal Declaration of Human Rights, 10 December 1948, GA res. 217A (III), UN Doc A/810 at 71 (1948).

23 Universal Declaration of Human Rights, *supra* note 23, Article 12.

24 Declaration of Principles on Freedom of Expression in Africa, *supra* note 18, Principle I.

Declaration on Principles of Freedom of Expression in Africa

Principle I of the African Commission's Declaration on Principles of Freedom of Expression in Africa (the "Declaration") defines the right to freedom of expression and information as "including the right to seek, receive and impart information and ideas, either orally, in writing or in print, in the form of art, or through any other form of communication, including across frontiers, is a fundamental and inalienable human right and an indispensable component of democracy."[25]

Principle II of the Declaration states that "Any restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary and in a democratic society."[26] Principle XIII further states that "Freedom of expression should not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression."[27]

The specific inclusion of all forms of communication and the echoing of the three-part test found in the ICCPR and African Charter confirm the applicability of these standards to online expression in Uganda.

African Declaration on Internet Rights and Freedoms

The African Declaration on Internet Rights and Freedoms is "a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent."[28] Principles 3 and 8 of the Declaration emphasize that any restriction of the right to freedom of expression or the right to privacy on the internet must be subject to the three-part test.[29]

---

25 Declaration of Principles on Freedom of Expression in Africa, supra note 18, Principle II.

26 Declaration of Principles on Freedom of Expression in Africa, supra note 18, Principle XIII.

27 African Declaration on Internet Rights and Freedoms, 4 September 2014.

28 "This right should not be subject to any restrictions, except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law", African Declaration on Internet Rights and Freedoms, supra note 28, Key Principle 3. Available at: http://africaninternetrights.org/articles/.

29 "Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognized under international law (the 'three-part' test)", Joint Declaration on Freedom of Expression and the Internet, 1 June 2011), General principle 1a.

Joint Declaration on Freedom of Expression and the Internet

The Joint Declaration on Freedom of Expression and the Internet, made by the UN Special Rapporteur, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the African Commission Special Rapporteur on Freedom of Expression and Access to Information, states that freedom of expression applies to the internet, and reiterates that restrictions on online expression are acceptable only if they comply with the three-part test.[30]

International Principles on the Application of Human Rights to Communications Surveillance (Necessary & Proportionate)

The three-part test is an integral part of other international standards related to privacy. The International Principles on the Application of Human Rights to Communications Surveillance are the "product of a year-long consultation process among civil society, privacy and technology experts" launched by the UN Human Rights Council in Geneva in September 2013.[31] The Principles elaborate on the three-part test, and additionally state that specific instances of communication surveillance must be authorized "by a competent judicial authority that is impartial and independent."[32] In addition, the Principles also require those whose communications are being surveilled to be notified "with enough time and information to enable them to challenge the decision or seek other remedies." States are also required to be more transparent regarding the use and scope of communications surveillance laws and activities, and to "establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance."[33]

30 Necessary and Proportionate Coalition, Necessary & Proportionate ("Necessary & Proportionate"), May 2014, available at http://necessaryandproportionate.org/principles.

31 Necessary & Proportionate, supra note 31, Principle 6.

32 Id.

33 African Commission on Human and Peoples' Rights, Resolution on the Right to Freedom of Expression on the Internet in Africa, 4 November 2016, ACHPR/Res. 362(LIX) 2016.

Resolution on the Right to Freedom of Information and Expression on the Internet in Africa

The African Commission's Resolution on the Right to Freedom of Expression on the Internet in Africa was adopted on 4 November 2016.[34] The resolution reaffirms the right to freedom of information and expression enshrined in Article 9 of the African Charter and "other international human rights instruments", including the Declaration of Principles on Freedom of Expression in Africa, and takes note of the African Declaration on Internet Rights and Freedoms.[35]

The Resolution recognizes "the importance of the Internet in advancing human and peoples' rights in Africa, particularly the right to freedom of information and expression."[36] It further recognizes that "privacy online is important for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."[37] Additionally, it recalls the UN Human Rights Council Resolution of 2012 which affirms that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[38]

34 Id.
35 Id.
36 Id.
37 Id.
38 Article 19, Submission to the UN Universal Periodic Review For consideration at the twelfth session of the UPR Working Group, October 2011.

II. COMPLIANCE OF SPECIFIC UGANDAN STATUES WITH INTERNATIONAL STANDARDS ON FREEDOM OF EXPRESSION AND THE RIGHT TO PRIVACY

A. Regulation of Interception of Communications Act, 2010

The Regulation of Interception of Communications Act ("RICA") lacks adequate safeguards to ensure protection of freedom of expression and the right to privacy. RICA gives the government unduly broad discretion to monitor and intercept electronic, telecommunications, and postal communications between individuals, groups, and organizations. RICA's vague and excessively permissive basis for intercepting communications contravenes international standards—such as by sanctioning intrusions into the communications of individuals engaged in exercising their human rights.[39]

Key Recommendations

- The definition of "national security of Uganda" in Section 1 must be more narrowly and precisely defined to avoid arbitrary interpretation and application by authorities;
- Procedures for the judicial authorization of interception warrants must be made explicit in Section 5 to ensure interceptions are truly necessary and always proportionate;
- "National economic interest" should be removed from Section 5(1)(c) and (d) as grounds for the interception of communications.
- Provisions must be put in place to protect the privacy of SIM card users who are required to turn over personal information under Section 9;
- The disclosure of information under Section 10 should occur only pursuant to a judicial warrant, in line with the procedures recommended for Section 5;
- "National economic interest" should be removed from Section 10(b)(iv) as grounds for the interception of communications.

39 General Comment 34, supra note 8, Para. 25. f it turns out to be too challeh the MENA online platform?ing the training programme elsewhere if it turns out to be too challe

Analysis

Section 1 of RICA defines the "national security of Uganda" as including "matters relating to the existence, independence or safety of the State."

As set out in Section I.A above, the UNHRC has stated that "[a] law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[40] The UN Special Rapporteur has raised concerns about the amorphous concept of national security, noting that authorities can manipulate the concept to justify targeting vulnerable groups like human rights defenders, journalists, or activists. According to the UN Special Rapporteur, the concept also allows for unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.[41] RICA's definition of "national security of Uganda" is overly broad and open to interpretation, violating the requirement that any restriction on the right to freedom of expression must be provided by law. The provision needs to be revised so that it is more precisely and narrowly defined.

As set out in Section I, International norms state that any restrictions on the right to privacy must be prescribed by law, pursue a legitimate aim, and conform to the tests of necessity and proportionality.[42] The test of necessity stipulates that any surveillance or interception activity "must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim."[43] Therefore, such activities should be authorized only as a last resort.

Section 5 of RICA falls short of these norms. According to Section 5(1), a warrant for interception of communications will be issued to authorities if there are reasonable grounds for a designated judge to believe that:

> "(a) an offence which may result to loss of life or threat to life has been or is being or will probably be committed;
>
> (b) an offence of drug trafficking or human trafficking has been or is being or

40 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, supra note 14, par 60.

41 Necessary & Proportionate, supra note 31.

42 Id.

43 Regulation of Interception of Communications Act, Section 5(1).

will probably be committed;
(c) the gathering of information concerning an actual threat to national security or to any national economic interest is necessary;
(d) the gathering of information concerning a potential threat to public safety, national security or any national economic interest is necessary; or
(e) there is a threat to the national interest involving the State's international relations or obligations."[44]

These provisions are inconsistent with international standards, for the following reasons.

First, the UN Special Rapporteur has noted that the burden of proof to establish the necessity for surveillance under RICA is "extremely low, given the potential for surveillance to result in investigation, discrimination or violations of human rights."[45] This is compounded by the absence of any requirement that surveillance be conducted as a last resort. As a result, the provision as written allows for authorities to obtain a warrant to intercept communications so long as they minimally justify it under the delineated grounds. This contravenes the international principle that surveillance activities be authorized as a last resort.

Second, there are no explicit provisions or criteria in RICA for a judge to consider and apply before issuing a warrant for interception of communication. This means that a judge is not required to weigh any potential human rights violations before issuing a warrant, which increases the risk that warrants for interception could result in a violation of the right to privacy.[46] Furthermore, any warrants issued may not conform to international standards with regards to the need to ensure that government action taken in relation to interception and monitoring of communications is necessary and proportionate.[47]

44 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, supra note 14, par. 56.
45 Amnesty International, Memorandum on the Regulation of Interception of Communications Act, 2010, AFR 59/016/2010, 14 December 2010.
46 Necessary & Proportionate, supra note 31.
47 Regulation of Interception of Communications Act, Sections 5(1)(c) and (d).

Third, the lack of precise procedures allows for a broad interpretation of RICA, allowing for potential abuse. To bring this provision in line with international standards, the procedures for judicial authorization must be made explicit to ensure any interception is necessary and proportionate to the aims described.

Fourth, and finally, Sections 5(1)(c) and (d) mention "any national economic interest" as possible grounds for the interception of communication.[48] However, this is not a legitimate aim for restricting the right to privacy under international law and should therefore be removed.

Section 9 requires telecommunications companies to register the users of SIM cards. There are concerns that this compromises the communications anonymity of users and impacts the privacy of individuals who use mobile phones by making it easier to intercept the communications and track the physical location of identified individuals.[49] In addition, telecommunications companies often have terms and conditions that could permit handing collected user data over to authorities upon government request.

The right of anonymity of communications protects individuals' ability to exercise the rights of free expression, assembly, and association. In addition, ICCPR Article 17(1) protects the privacy of correspondence. Requiring the registration of personal information of SIM card users without any legitimate grounds or requirements constitutes an arbitrary interference with the privacy of correspondence. Provisions must be set in place to safeguard the privacy and right to anonymous communications of SIM card users who are required to provide personal information under this Article.

48 CIPESA, Privacy in Uganda: An Overview of How ICT Policies Infringe on Online Privacy and Data Protection, CIPESA ICT Policy Briefing Series No. 06/15, December 2015.

49 Regulation of Interception of Communications Act, Section 10(1).

Section 10 permits authorities to require the disclosure of protected information, defined as "information that is encrypted by means of a key", if they believe on reasonable grounds that:

"(a) that a key to any protected information is in the possession of any person; and

(b) that the imposition of a disclosure requirement in respect of the protected information is necessary—

(i) in the interest of national security; or

(ii) for the purpose of preventing or detecting an offence that may result to loss of life or threat to life; or

(iii) for the purpose of preventing or detecting an offence of drug trafficking or human trafficking; or

(iv) in the interest of the economic well-being of Uganda;

the 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."[50]

Much like Section 5, these are overly broad and poorly defined criteria for accessing protected information. Section 10 needs to be more narrowly and precisely defined. In addition, Section 10(b)(iv) should be removed, as economic interests are not legitimate aims for limiting people's right to privacy.

Unlike Section 5, Section 10 does not explicitly require judicial authorization. Authorities may therefore interpret the provision to infer that such judicial authorization is not necessary to compel the disclosure of protected information, leaving open the possibility that authorities may seek such information without first obtaining a judicial warrant. Because the provision does not place any checks on authorities' ability to compel disclosure, there is an increased risk that authorities may abuse this provision and violate an individual's right to freedom of expression and right to privacy.[51] The requirement of obtaining a judicial warrant should be clearly specified in Section 10.

50 Amnesty International, Memorandum on the Regulation of Interception of Communications Act, supra note 46.

51 Anti-Terrorism (Amendment) Bill, 24 April 2015.

B. Anti-Terrorism Act, 2002

Uganda amended the Anti-Terrorism Act of 2002 ("Anti-Terrorism Act") in 2015 to expand definitions of criminalized acts, make "indirect" involvement in terrorist activity subject to the same penalties as other criminalized acts, and include provisions criminalizing interference with electronic systems and possession of materials promoting terrorism.[52] The Anti-Terrorism Act contravenes international standards of freedom of expression and the right to privacy due to its overly broad wording and lack of clear boundaries on the surveillance powers it establishes.

Key Recommendations

- The key offences of "terrorism" and aiding and abetting terrorism in Sections 7, 8, and 9 should be more narrowly defined to meet the requirement of legality under international law;
- Sentencing guidelines should be provided for the various classes of offences under the act to ensure the necessity and proportionality of the levied penalties;
- Section 19 should specify the circumstances in which each type of surveillance and investigation is appropriate to safeguard adherence to the principles of necessity and proportionality;
- Any order for the interception of communications under Section 19 must explicitly require judicial authorization;
- The reference to the protection of the national economy should be removed from Section 19(4).

Analysis

Section 7(2) defines "terrorism" very broadly to include, notably, "serious interference with or disruption of an electronic system" for purposes of "… for purposes of influencing the Government or intimidating the public or a section of the public and for a political, religious, social or economic aim, indiscriminately without due regard to the safety of others or property…."[53]

52 Anti-Terrorism Act, Section 7(2).
53 Anti-Terrorism Act, Section 8.

Further under Section 8, aiding and abetting terrorism is a punishable offense. This provision encompasses behavior including financing, harboring or supporting "any person, knowing or having reason to believe that the support will be applied or used for or in connection with the preparation or commission or instigation of acts of terrorism."[54]

These provisions are overly broad. Their wording may criminalize legitimate behavior, including the exercise of human rights such as the right to freedom of expression. For example, it is unclear what should be considered a "serious interference with or disruption of" an "electronic system," as none of the elements of the offence are further defined. Nor is it clear what qualifies as "influencing the Government ... for a political, religious, social or economic aim." Arguably, a range of legitimate activities, such as a successful campaign encouraging citizens to e-mail their parliamentarian on a matter of public concern which has the collateral effect of overloading government servers, could be captured under these provisions.

Section 9 violates the principle that legislation must be sufficiently precise to allow citizens to determine their behavior accordingly, as set out above in Section I of this memorandum. On anti-terrorism legislation, the UNHRC has stated specifically that:

> "States parties should ensure that counter-terrorism measures are compatible with paragraph 3 [of ICCPR Article 19]. Such offences 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."[55]

Section 9 includes precisely this type of wording, as it criminalizes "promoting" terrorism as well as "publishing and disseminating news or materials that promote terrorism."[56] As it is not clear what constitutes the "promotion" of terrorism, journalistic reporting on anything related to terrorism or terrorist organizations could potentially fall under this provision.

54 General Comment 34, supra note 8, para. 46.
55 Anti-Terrorism Act, Section 9.
56 Anti-Terrorism Act, Section 7(1)(a).

This gives unfettered discretion to the authorities to suppress legitimate reporting on matters of public interest, which in turn has a chilling effect on freedom of expression.

Sections 7, 8 and 9 should therefore be more narrowly and precisely defined so as to not unduly curtail the exercise of the right to freedom of expression.

These broadly defined offences under the Act carry heavy penalties, which can be considered disproportionate under international law.

Section 7(1)(a) mandates the death sentence for offences under the Act if those result in "the death of any person,"[57] while Section 7(1)(b) makes the death penalty available for any other offence under the Act.[58] As the definition of "terrorism" is overbroad, as set out above, Section 7 allows the death penalty to be imposed both for minimal infractions, and for conduct that constitutes a legitimate exercise of person's human rights. The UNHRC observed in General Comment No. 27 that:

> "restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law."[59]

The Act should make a clear distinction between the different categories of offences and the penalties that can be incurred to ensure sanctions are proportionate and necessary to further the legitimate interests of the Act.

Under Section 18(1) the Minister for Internal Affairs "… may, by writing, designate a security officer as an authorized officer [who, under provision 19(1)] shall have the right to intercept the communications of a person and otherwise conduct surveillance of a person under this Act."[60]

57 Anti-Terrorism Act, Section 7(1)(b).
58 General Comment No. 27, supra note 10, par. 14.
59 Anti-Terrorism Act, Section 18(1).
60 Anti-Terrorism Act, Section 19(4).

The Minister may therefore unilaterally authorize the interception of communications and surveillance.

Section 19(4) sets out the conditions for authorization, which include: "… 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 this Act, [and] safeguarding the national economy from terrorism."[61]

These provisions are overly broad and give unfettered discretion to the Minister to order the interception of communications, without having to demonstrate the necessity or proportionality of such measures. In particular, the extension of this power to detecting the commission of "any" offense is of concern, because the provision does not clearly explain what the legal or factual basis should be for authorizing the interception of communications or surveillance of an individual. This is aggravated by the overly broad definition of offences under the Act, as described above. Furthermore, safeguarding the national economy is not a legitimate aim to restrict the right to privacy, as set out above in Section I. This phrasing should therefore be removed from Section 19(4).

Under Section 19(5), the authorization covers:

"The interception of letters and postal packages of any person … interception of the telephone calls, faxes, emails and other communications made or issued by or received by or addressed to a person… monitoring meetings of any group of persons … surveillance of the movements and activities of any person … electronic surveillance of any person … access to bank accounts of any person … searching of the premises of any person".[62]

61 Anti-Terrorism Act, Section 19(5).
62 Anti-Terrorism Act, Section 19(6).

Further, the authorized officer has:
"The right to detain and make copies of any matter intercepted by the authorized officer … the right to take photographs of the person being surveilled and any other person in the company of that person, whether at a meeting or otherwise … the power to do any other thing reasonably necessary for the purposes of this subsection."[63]

The existence of surveillance practices in and of itself has a chilling effect on the right to freedom of expression.[64] In the words of the UN Special Rapporteur: "Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.[65] … States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy."[66]

The centralized power to authorize surveillance given to the Minister under the Act, in combination with the breadth of this investigative and surveillance power, is rife with the possibility of abuse and contravenes the right to privacy and freedom of expression. This is aggravated by the lack of a judicial authorization or review mechanism for orders to intercept communications. The Act should clearly delineate the circumstances in which each type of surveillance and investigation is appropriate to safeguard adherence to the principles of necessity and proportionality. It should also impose a judicial authorization requirement for all communications surveillance to ensure a balancing of the legitimate interest of combatting terrorism with considerations of privacy and free expression takes place.

63 Necessary & Proportionate, supra note 31.
64 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, supra note 14, par. 52.
65 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, supra note 14, par. 79.
66 Anti Pornography Act, Section 13.

C. Anti Pornography Act, 2014

The Anti Pornography Act, 2014 ("Anti Pornography Act") makes it an offence to produce, participate in the production of, traffic in, publish, broadcast, procure, import, export, or in any way abet any form of pornography.[67] On conviction, a person is liable to a fine of up to five hundred currency points,[68] or imprisonment up to ten years, or both.[69] In its preamble to the Anti-Pornography Bill, the Ugandan Parliament explains that the law "seeks to create the offence of pornography which is blamed for sexual crimes against women and children including rape, child molestation and incest."[70]

Regardless of its purported purpose, the Act imposes restrictions in a manner that contravenes international standards on freedom of expression and the right to privacy due to an overbroad definition of "pornography", the granting of unlimited discretionary power to the Pornography Control Committee ("the Committee"), and an excessive imposition of intermediary liability on internet service providers ("ISPs").

67 A currency point is equivalent to twenty thousand Ugandan shillings. Anti-Pornography Act, Schedule 1.

68 Anti Pornography Act, Section 13.

69 Parliament of the Republic of Uganda, Parliament passes Anti-Pornography Law, 2014. Published on: http://www.parliament.go.ug/new/index.php/about-parliament/parliamentary-news/325-parliament-passes-anti-pornography-law.

70 Anti Pornography Act, Section 2.

Key Recommendations

- The definition of "pornography" in Section 2 should be redefined with greater precision to limit the scope of representations that are criminalized and prevent the suppression of legitimate forms of expression, discrimination against women, and undue restriction of cultural practices;
- Section 11 should be repealed entirely. Alternatively, the investigative powers of the Committee under Sections 11(a), (b), (c), (d), and (e) should be made subject to a judicial warrant and clear guidance should be provided on when the Committee can employ which enforcement measures;
- Section 11 should be struck in its entirety to prevent ISPs from bearing responsibility for accessing and distributing illegal content;
- Section 11(g) should limit the scope of authorized arrest to ensure the necessity and proportionality of this measure;
- The prohibited acts in Section 13 must be clearly and narrowly defined to enable individuals to anticipate the Act's scope, and to provide exceptions for intermediaries;
- Section 17 should be repealed and replaced with a provision that immunizes ISPs and other intermediaries from any liability for facilitating the transmission of pornographic or other illegal content.

Analysis

Section 2 of the Anti Pornography Act defines "pornography" as:

> "any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual excitement."[71]

This definition of "pornography" is too vague to be provided by law, and arguably does not have a legitimate aim as required under international law. Consequently, it fails to meet the strict requirements under which freedom of expression can be restricted under the ICCPR and African Charter.

71 General Comment 34, supra note 8, par. 25.

First, the definition of "pornography" is not "provided by law," as it is both impermissibly vague and overbroad. As the UNHRC has stated, a norm "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. . ."[72] The definition fails this precision requirement, as individuals cannot reasonably determine what expression the statute prohibits, leaving them vulnerable to arbitrary determinations by the authorities of what is criminal. The definition also fails to state with precision what constitutes a "sexual part," and provides no guidance on what kinds of expression are "for primarily sexual excitement." Additionally, the definition's sweeping "any representation" language has the potential to capture forms of expression that are not commonly considered pornography, such as an individual's choice of clothing.

Taken together, the vague definition of "pornography" creates not only the potential for arbitrariness in determining whether a particular "representation" is forbidden, but it risks criminalizing legitimate forms of expression, such as works of cultural, artistic, or scientific merit. Section 2 should therefore be more precisely defined.

Second, the vague and overbroad definition of "pornography" causes the Act to deviate from what can be considered a legitimate purpose for the restriction of freedom of expression. While ICCPR Article 19 recognizes the legitimacy of restrictions on free expression for the protection of "public health or morals,"[73] such restrictions must conform with the non-discrimination principle of the ICCPR. They must therefore "be understood in the light of universality of human rights and the principle of non-discrimination,"[74] and guarantee "equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[75] This includes protection of the right of persons belonging to minority groups to "not be denied the right, in community with the other members of their group" and "enjoy their own culture..."[76]

72 International Covenant on Civil and Political Rights, supra note 1, Article 19.
73 General Comment 34, supra note 8, par. 32.
74 International Covenant on Civil and Political Rights, supra note 1, Article 26.
75 International Covenant on Civil and Political Rights, supra note 1, Article 27.
76 BBC, Uganda miniskirt ban: Police stop protest march, 26 March 2014. Published on: http://www.bbc.com/news/world-africa-26351087.

The Anti Pornography Act's vague definition of "pornography" can and has been interpreted in a discriminatory manner. The Act's provisions have been construed to apply to what women wear, earning it the moniker the "Miniskirt Law."[77] Simon Lokodo, Minister of Ethics and Integrity, explained to the press that the Act outlaws "any indecent dressing" that "exposes intimate parts of the human body" as pornographic representations.[78] Lokodo vowed that "women wearing clothing that stopped above their knees" would be arrested.[79] Lokodo's discriminatory interpretation of the law may not be binding, but it is nonetheless likely to prove influential, as the Act empowers the Minister to appoint members of the Pornography Control Committee.[80] The Committee, in turn, are tasked with enforcing the Act through lawmaking, inspections, seizures, and arrests through police officers.[81]

The practical discriminatory effects of Minister Lokodo's interpretation have been seen on the streets of Uganda, when mobs of men, citing the Anti Pornography Law, stripped clothing deemed to be "indecent" off of women.[82] Since the passage of the Act, 44 such assaults on women have been recorded in Kampala alone.[83] While the police warned the public against undressing women, they also instructed them to "report to Police" when they "suspect that [a] person is indecently dressed," thereby implicitly endorsing an interpretation of the law that discriminates against women in contravention of the ICCPR.[84]

77 The Guardian, Uganda proposes ban on miniskirts in move against women's rights, 5 April 2013. Published on: https://www.theguardian.com/world/2013/apr/05/uganda-ban-miniskirts-womens-right.

78 Ivan Seguya, The Anti-Pornography Act in Uganda Through the Gender Lens, 2014. Available at: http://independent.academia.edu/ivanseguya.

79 Anti-Pornography Act, Section 3.

80 Anti-Pornography Act, Section 11.

81 Wits Journalism, Uganda's anti-pornography law targets media more than miniskirts, 9 March 2014. Published on: http://www.journalism.co.za/blog/ugandas-anti-pornography-law-.

82 Strategic Initiative for Women in the Horn of Africa (SHIA), Anti-Pornography Act – Human Rights Activists and Civil Society Organisations Challenge the Legality of the Act in Constitutional Court. Published on: http://sihanet.org/news/anti-pornography-act-human-rights-activists-and-civil-society-organisations-challenge-legality.

83 Daily Monitor, Anti-pornography law: Police warns against undressing women, 25 February 2014. Published on: http://www.monitor.co.ug/News/National/Anti-pornography-law--Police-warns-against-undressing/-/688334/2220210/-/omy4tbz/-/index.html.

84 See Seguya, supra note 79.

Furthermore, applying the law as Minister Lokodo has interpreted it would criminalize the way of life of several traditional cultures in Uganda. For instance, in the Karamajong community, "moving naked is seen as a normal way of life."[85] A law that criminalizes the cultural practices of an entire community is in flagrant violation of Uganda's international obligations under international law and therefore cannot stand.

For all these reasons, "pornography" should be redefined with greater precision in Section 2 to limit the scope of representations that are criminalized, thereby preventing the suppression of legitimate forms of expression, discrimination against women, and undue restriction of cultural practices.

Section 11 grants the Pornography Control Committee, created under Section 3,[86] the ability to, "in the performance of its duties under the Act or any regulations made under the Act, at all reasonable times and without warrant –

(a) require production, inspection and examination of records and any other necessary documentation relating to enforcement . . .;
(b) carry out inquiries to ensure that this Act is complied with;
(c) carry out periodic inspection of any establishment…that is likely to give the public access to pornography;
(d) carry out inspections as may be necessary to ensure that the provisions of this Act are complied with;
(e) seize any equipment, document, or any other thing which it believes has been used in the commission of an offence against this Act or regulations made under this Act;
(f) close any internet service provider who promotes, publishes, sells or imports pornography contrary to this Act; or
(g) cause a police officer to arrest any person whom it believes has committed an offence under this Act."[87]

85 Anti Pornography Act, Section 3.
86 Anti Pornography Act, Section 11.
87 General Comment 34, supra note 8, par. 33.

These provisions fall short of the international human rights standards that bind the Ugandan government, in the following respects.

First, Section 11 grants the Committee the authority to conduct searches and inspections "without warrant". This cannot be considered "provided by law" because it confers the Committee with unlimited discretion. Under Section 11's terms, the Committee is empowered to raid every establishment and inspect every smartphone in Uganda, if it "believes" these are somehow implicated in the viewing of what Section 2 defines to be pornographic. Such unchecked powers pose not only a threat to the right to freedom of expression and privacy, but they are inconsistent with the very ideas of democracy and the rule of law. Section 11 should therefore either be repealed entirely, or the investigative powers that Sections 11(a), (b), (c), (d), and (e) grant the Committee should be subject to the issuance of a warrant by a neutral and independent magistrate.

Second, Sections 11(e), 11(f), and 11(g) enable the Committee to take enforcement measures that are neither necessary nor proportionate to those aims of the Act that can be considered legitimate. Per the UNHRC, a law violates the test of necessity if "the protection could be achieved in other ways that do not restrict freedom of expression"[88] and violates the test of proportionality if it is not "the least intrusive instrument amongst those which might achieve their protective function."[89] However, these provisions empower the Committee to take extraordinarily broad enforcement measures with no regard of their necessity or proportionality. Guidance on which measures can be employed under which circumstances should be included in the Act.

Section 11(e) empowers the Committee to seize "any equipment, document, or any other thing" believed to have been used in a violation of the Act or the regulations made under it. No matter how minor a role the "thing" in question played in violating the Act's provisions, the Committee is vested with the power to seize it. Hence, a bank might have its computers seized because an employee misused it to watch pornography, or a mobile communications provider might have all of their equipment

88 General Comment 34, supra note 8, par. 34.
89 Anti Pornography Act, Section 13.

seized because one subscriber downloaded pornography over their network. These measures are completely excessive, especially since there are no checks whatsoever on the Committee's powers. They are rife with the potential to be abused by the members of the Committee to conduct unjustified searches and seizures for purposes other than enforcing the Act's provisions. Consequently, Section 11(e) should either be repealed, or the Committee should be required to obtain a judicial warrant before seizing or searching the instrumentalities of pornography.

Section 11(f) allows the Committee to shutter Internet Service Providers ("ISPs") when they promote, publish, sell, or import "pornography" as currently (over-broadly) defined in Section 2. The vague wording of the provision appears to give the Committee the unfettered discretion to shut down an ISP that is unintentionally involved in the distribution of pornography, such as by "importing" a pornographic image into Uganda when a user clicks on a link. Considering the crucial role that ISPs play in citizens' ability to exercise their right to freedom of expression and right to information, this provision should be struck in its entirety. Responsibility for accessing and distributing illegal content, whether pornography or something else, should be borne by the individual user and not by the ISP to be consistent with international human rights standards.

Section 11(g) empowers the Committee to cause the arrest of any person who it believes to have committed an offence under the Act. Thus, the Committee could order the arrest of an individual for the most minor of infractions–such as unknowingly abetting the distribution of content that lies at the fringes of what could be considered pornographic–on the most minimal of evidentiary records. Section 11(g) should limit the scope of authorized arrest to ensure that it occurs only when the circumstances make it essential to the enforcement of the law, and when there is significant evidence to suggest that the individual has in fact violated the law.

Section 13 of the Anti-Pornography Act states that:

(1) A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography.

(2) A person who produces or participates in the production of, or traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography contrary to subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding ten years or both.[90]

The lack of precision in the definition of "pornography" in Section 2 is compounded by the breadth of what Section 13 prohibits. While "traffic," "publish," and "broadcast" are defined in Section 2, the remaining terms are undefined in Section 13.[91] The definition of "traffic" in Section 2 is so broad that it not only distorts the ordinary meaning of the word, but it encompasses such a broad spectrum of acts that Section 13 is likely to criminalize legitimate speech and behavior, in contravention of the ICCPR.[92] Additionally, the prohibition of "sell[ing]" creates the threat of criminal liability for innocent intermediaries—from bookshops to ISPs—who cannot possibly examine all of the material that passes through their establishments for compliance with Section 2's impermissibly vague definition of pornography. In conjunction with the redefinition of "pornography" in Section 2, the prohibited acts in Section 13 must be clearly defined and sufficiently limited to enable individuals to anticipate the Act's scope, and to provide exceptions for intermediaries who cannot practically monitor all of the content that they handle.

90 See Anti Pornography Act, Section 2.

91 "Traffic" is defined as "to deal in or cause or permit or aid the provision or circulation of pornographic matter by way of trade or publishing or entertainment or programming or unrestricted internet access or any other means or purpose", Anti Pornography Act, Section 2.

92 Anti Pornography Act, Section 17.

Section 17 provides that:

(1) An Internet Service Provider (ISP) who, by not using or enforcing the means or procedure recommended by the Committee 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.

(2) Where a publisher or broadcaster or internet-content-developer or dealer in telephone-related business or Internet Service Provider (ISP) commits an offence under subsection (1), the court convicting that person may, for a subsequent offence, by order, suspend the business.

(3) A person who fails to comply with an order given under subsection (2) commits an offence and is liable on conviction to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding five years or both.[93]

Section 17(1), which holds ISPs liable for permitting "any content of a pornographic nature,"[94] is at odds with international human rights standards. Since ISPs cannot realistically completely prevent the transmission of such content,[95] Section 17(1) coerces them into implementing whatever censorship scheme the Committee determines, on pain of facing large fines or even imprisonment.

Section 17(2)'s authorization of court orders to suspend the operations of an ISP for permitting pornographic content to be uploaded or downloaded is unnecessary, disproportionate, and in contravention of international standards. Per the UNHRC, "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, are only permissible to the extent that they are compatible with [Article 19] paragraph 3."[96] Shutting down an intermediary ISP for allowing the transmission of a single

93 Anti Pornography Act, Section 17.

94 Global Network Initiative, Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose, March 2014.

95 General Comment 34, supra note 8, par. 43.

96

representation of "pornography" (as impermissibly broadly defined in Section 2) is wholly disproportionate, especially considering the important role of ISPs in citizens' right to freedom of expression and right to information.

Section 17 should be repealed and replaced with a provision that immunizes ISPs and other intermediaries from any liability for facilitating the transmission of pornographic or other illegal content, consistent with the fundamental legal principle that the individual who accesses illegal content should be responsible for the consequences of so doing.

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