HRNJ-UGANDA

WEB WE WANT

Analysis of the Computer Misuse Act 2011

Analysis
of the
Computer Misuse Act
2011

Human Rights network for Journalists- Uganda

HRNJ-UGANDA

WEB WE WANT

TABLE OF CONTENTS:

ABOUT US	3
Vision	3
Mission	3
ACKNOWLEDGMENT	5
1.0 INTRODUCTION	6
2.0 UNNECESSARY LIMITATION AND CRIMINALIZATION OF ACCESS TO INFORMATION	9
3.0 INFRINGEMENT ON THE RIGHT TO PRIVACY	14
4.0 VAGUE AND AMBIGOUS SECTIONS IN THE LAW	19

ABOUT US

Vision

The vision of HRNJ-U is "An informed and respectful society of human rights free from abuse"

Mission

HRNJ-U contributes to the realization of its vision by enhancing the promotion, protection and respect of journalists rights through strengthening capacity strengthening for collective advocacy. HRNJ-U mission is; enhancing the promotion, protection and respect of human rights through defending and building capacities of journalists to effectively exercise their constitutional rights and fundamental freedoms for collective campaigning through the media.

HRNJ-U undertakes urgent efforts to energize journalists into a strong critical mass capable of influencing the human rights agenda as well as act in defense of overall human rights violations.
HRNJ-U was established in 2005 by a group of human rights minded journalists who developed a sense of activism amidst a deteriorating context due to glaring violations and abuses targeting the media. The Network gained formal registration as an independent non profit and non partisan media organization in 2006. The identity of HRNJ-U lies with its diverse membership across board including the print and electronic media, freelance investigative journalists and individuals from other professions.
Programmes

Under her strategic plan HRNJ-U devotes her efforts, energy and resources to:(1) Advocacy and Networking: The Network undertakes advocacy campaigns to influence the legal and policy issues pertinent to the oversight role enjoyed by the media in Uganda (2) Capacity Building & Network Development: This programme involves strengthening skills and capacity of HRNJ-U staff, members volunteers, interns, journalism and mass communication students. It also involves conducting exchange fellowships for experience sharing and learning. (3) Legal Aid and Support: The programme entails offering free legal service to journalists and members of society who are victimized for excercising free speech and expression. (4) Research and Documentation: This entails undertaking research and documenting human rights violations, monitoring and reporting to treaty and regional bodies about the country's performance in regard to international human rights instruments and (5) Institutional Development, Finance and Adminstration: This programme area entails strengthening the operational and policy context with the purpose of strengthening institutional systems, structures and programmes in order to enhance output.

ACKNOWLEDGMENT

The law was analysed by lead lawyer Isaac Kimaze, Haruna Kanaabi and the HRNJ-U legal team comprised of Anite Catherine the Programme Officer and Diana Nandudu the deputy. HRNJ-U wishes to appreciate their tireless contribution to this process. We are also indebted to the Web-We-Want for extending the support to have this analysis undertaken without which it would not have been possible. And, also our appreciation goes to staff of HRNJ-U led by Mr. Robert Ssempala, the National Coordinator and the Capacity building Programme Officer for their selfless input to this process

1.0 INTRODUCTION

Government of Uganda is increasingly facilitating its citizens to seek, receive and impart information through the development of information and communication technology policies and structures. In early 2000, a ministry of information and communication technology was created to: "provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy for the ICT sector; sustainable, effective, and efficient development, harnessing and utilization of ICTs in all spheres of life to enable the country to achieve its development goals."[1]

In an effort to promote use of information and communication technology, the government exempted import duty on computers to increase affordability, started a program of giving computers to all government aided schools and is increasingly encouraging students to study computer.

However, access to a computer per person and internet remains very low in the country. According to Ministry of ICT, "There is very low computer penetration, with the urban areas having over 80% of the computer penetration in the country. The computer penetration is higher in government than in the private sector".[2]

Despite all these efforts, the legal framework to facilitate the full enjoyment of ICT is non comprehensive, overly vague and broad in context, a fact acknowledged by the government. "The country still

1 Ministry Of Information And Communications Technology Ministerial Policy Statement Vote: 020 Financial Year 2012/2013

2 Ibid

has a very weak legislation pertaining to this industry. Laws related to Intellectual Property Rights, Data Security, Privacy, Data Protection and cyber crimes are still in infancy and where they exist, enforcement is still low and others are outdated. The existing Acts need to be amended to address the gaps which have been identified."[3]

Besides, there is lack of appreciation of Information Technology in many "sectors as a strategic unit of economic transformation by both the private and public sector."[4] Efforts have been made to formulate laws and policies to regulate Information Technology. Although the government has the intention to "ensure access to Information Technology services to men and women in both rural and urban areas,[5]" the laws put in place do not entirely conform to this school of thought.

The Constitution of the Republic of Uganda guarantees freedom of expression, access to information and the right to privacy.[6] Uganda is also a party to international and regional instruments like the Universal Declaration of Human Rights (UDHR)[7], International Covenant on Civil and Political Rights (ICCPR)[8] and African Charter on Human and People's Rights[9] which set clear standards on enjoyment

3 Information Technology Policy for Uganda, September 2012
4 Ibid
5 ICT Policy
6 Constitution of Uganda Chapter 4. Article 29 (1)(a) guarantees freedom of expression and Article 43 specifies the limitations and restrictions to this freedom
7
8 Article 19 of the ICCPR: Freedom may restrict to ensure respect for the rights or reputation of others and for the protection of National security or of public order, or public health or morals. Where a sate imposes certain restriction on the exercise of the freedom these must not be put in jeopardy. Such restriction must satisfy the condition laid down in Article 19(3)
9 Article 9(2) African Charter: Every individual shall have the right to express and

and restrictions on freedom of expression, privacy and access to information. Uganda is a partner state of the East African Community which requires member States to adhere "to universally acceptable principles of good governance, democracy, the rule of law, observance of human rights and social justice." [10]

In February 2011, the Parliament of Uganda enacted the Computer Misuse Act for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provisions for securing the conduct of electronic transactions in a trust worthy electronic environment.

However, the Computer Misuse Act poses imminent danger to free access to information, right to privacy, freedom of expression and a bundle of other rights. It contains ambiguous, vague, imprecise, sweeping, broad and confusing provisions that have potential to gravely affect the enjoyment of rights. Whereas the government is allowed to limit the enjoyment of freedoms, the restrictions must be narrowly defined and should conform to international standards of which Uganda is a party. The Computer Misuse Act falls short of these standards.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression appealed to governments all over the world "to adopt laws and regulations that allow people to communicate freely over the Internet and to remove all present

disseminate his opinions within the law

10 East African Treaty Article 3(3)(b)

obstacles to the free flow of information."[11]

2.0 UNNECESSARY LIMITATION AND CRIMINALIZATION OF ACCESS TO INFORMATION

2.1 Access to information is a nationally and internationally guaranteed right that must be enjoyed without undue interference. Article 41 of the Constitution of the Republic of Uganda guarantees the right to access to information in the hands of the state: (1) 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 is likely to prejudice the security or sovereignty of the State or interfere with the right to the privacy of any other person.

Article 19 of the Universal Declaration of Human Rights provides 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 41 (1) of the Constitution of the Republic of Uganda spells out clearly the limitation of access to information that it can only be withheld if the release is likely to prejudice the security or sovereignty of the state or interfere with the right to privacy. Article 41 (2) of the Constitution of the Republic of Uganda allows Parliament to enact

11 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and
expression" ("1998 Report"), p. 13, E/CN.4/1998/40, Jan. 28, 1998, available at http://www2.ohchr.org/english/issues/opinion/annual.htm.

laws classifying information and procedures of access: Parliament shall make laws prescribing the classes of information referred to in clause (1) of this Article and the procedure for obtaining access to that information.

Laws enacted must be in conformity with the Constitution of the Republic of Uganda, aimed at promoting, protecting and facilitating the enjoyment of rights as enshrined in the Constitution. Internationally accepted standards demand that the limitations provided for in the law must be narrowly defined and serve a broader purpose for the good of society but not a particular government, section of society or an individual.

Article 19 of the International Covenant on Civil and Political Rights of which Uganda is a state party offers good guidelines on accessing information and the circumstances under which access can be limited:

1. Everyone shall have the right to hold opinions without interference.
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.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order or of public health or morals.

2.2 Sections 5, 12 and 18 of the Computer Misuse Act unduly limit access to information in a broad manner and do not conform to the standards set out within the Constitution of the Republic of Uganda, Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The limitations set out in the Act do not serve any pressing social need; they are overly broad, unjustifiable and irrelevant.

2.3 According to Section 5 of the Act, access to information on the computer is allowed if consent is given:
Access by a person to any program or data held in a computer is authorised if—
(a) the person is entitled to control access to the program or data in question; or
(b) the person has consent to access that program or data from any person who is charged with giving that consent.

However the law lacks precise and proper procedures of accessing computers, (government or private owned), levels of access, how consent is given, when and why it should be denied. Considering the fact that most of the computers in Uganda are State owned and contain public information, it is unclear what recourse an aggrieved person has when consent is denied to access public information stored in a government computer. The procedure of seeking consent is not laid out in the law. Stipulations on what happens to an 'authorizing officer' who declines to consent to access a computer are lacking.

2.4 The Computer Misuse Act in section 12 and 18 without justifiable cause and classification of information broadly criminalizes access to information; restricts release of information and sets penalties of seven and ten years of imprisonment respectively. This contravenes the national Constitution and international standards. Section 12 of the law provides that:

(1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a manner that causes the program or data to be modified, damaged, destroyed or rendered ineffective, commits an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence.

(4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data, commits an offence.

(5) A person who accesses any information system so as to constitute a denial including a partial denial of service to legitimate users commits an offence.

(6) The intent of a person to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both. (One Currency point is equivalent to twenty thousand Uganda shillings, approximately eight U.S dollars).

2.5 Section 18 of the Act makes it an offence to release information and a person who does it is liable to imprisonment for ten years. It provides that:
(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, 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.
(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

These vaguely worded provisions create room for abuse of the right to access information and do not facilitate the enjoyment of rights. The law offers the government machinery a wider opening to deny citizens information in the hands of the State under the pretext of "unauthorized access" to computers.

3.0 INFRINGEMENT ON THE RIGHT TO PRIVACY

3.1 The right to privacy is guaranteed by the Constitution of the Republic of Uganda as well as other international human rights instruments. Article 27 of the Constitution of the Republic of Uganda states that:

(1) No person shall be subjected to: (a) unlawful search of the person, home or other property of that person; or (b) unlawful entry by others of the premises of that person

(2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

Article 12 of the Universal Declaration of Human Rights emphasizes the protection of the right to privacy. It provides 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.

Although it is none binding to countries, the UDHR offers good guidance to governments to formulate laws that protect the right to privacy. Further, Article 17 of the International Covenant on Civil and Political Rights provides that:

1. 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.

2. Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy has been extensively discussed by different bodies including courts and can only be interfered with for purposes of protecting another right. Governments are restricted from random and arbitrary interference with communication or correspondence of a person.

Human Rights Watch in its report 'False Freedom Online Censorship in the Middle East and North Africa' released in November 2005 examining internet freedom in the Middle East argued that:

"Freedom from arbitrary and unlawful interference with one's privacy and correspondence is protected both under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights and applies to electronic communications, including email and newsgroup postings, as well as electronic forms of personal data retained about individuals. Interference that is capricious, unjust or disproportionate would be "arbitrary," as would interference for a purpose inimical to the protection of human rights more generally, such as inhibiting peaceful dissent. States may not randomly or freely intercept or monitor email or Internet usage.

The United Nations Human Rights Committee, the treaty body that is an authoritative interpreter of state duties under the ICCPR, in a General Comment on the right to privacy, has said:

As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private

life the knowledge of which is essential in the interests of society as understood under the Covenant. […] Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. [….] Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

The right to privacy encompasses both the individual's right to a zone of autonomy within a "private sphere" such as the home, but also with respect to personal choices within the public sphere. This is important, as much of the controversy over how much respect to accord individual choices over Internet usage becomes caught up in characterizations of the Internet as a public space (e.g., a virtual town square or "information highway") or a zone of private communication or research (e.g., a telephone booth or a virtual library). Where the expectation of privacy also serves the purpose of facilitating freedom of expression and information, heightened scrutiny of government intrusion is appropriate. Such an expectation can be found in various contexts, such as attempts to protect the anonymity of an Internet "speaker," or the interests in keeping one's communications and browsing private even when using an Internet café. "

The veil on privacy can be lifted only if legitimate and necessary for the general good of society.

3.2 Sections 9, 10 and 11 of the Computer Misuse Act pose a serious threat to the right to privacy. Unlimited powers are granted to an 'investigative officer', not defined by law, to access data stored or processed by a computer for purposes of criminal investigations or prosecution of an offence.

These provisions further make it optional for an 'investigative officer' to apply for a court order to preserve, disclose and produce data as stipulated by the law. The discretion is therefore left to the 'investigative officer' to decide whether or not he or she finds it necessary to formally apply to court to access private information. Although the law under section 31 provides that a Chief Magistrate or Magistrate Grade One has jurisdiction to hear and determine offences within the Act, it is unclear which court has powers to grant the preservation, disclosure and production orders for release of information to the 'investigative officer'. The law is silent as to whether the application is oral or written.

3.3 Section 9(2) of the law allows the 'investigative officer' to intrude into personal privacy by defining data to include subscriber's information. Section 10 further grants the 'investigative officer' wide discretion to access data if a criminal investigation is being carried out or for prosecution of an offence. It provides:
The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or
(b) 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.

3.4 Section 11 (1) (a) and (b) of the Act gives powers to the 'investigative officer' to take the available information by force if the holder is unwilling to disclose it:
(1) 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—

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

In addition, section 11(2) of the law requires the holder of information to produce it in a manner that is visible and legible.
(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Such broad provisions and ambiguous terms like "all preserved data", "sufficient data", and "the request shall be deemed", within the law undermine the right to privacy without reasonable cause. Data put together and passed on to the 'investigative officer' as defined in the law gives access to the investigative officer to interfere with privacy as he or she attempts to find the necessary information he or she is looking for.

4.0 VAGUE AND AMBIGOUS SECTIONS IN THE LAW

4.1 The Computer Misuse Act contains vague and imprecise provisions that can be interpreted to the detriment of persons. The law broadly defines a computer as an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices.

The definition makes every gadget that stores or communicates data liable to the restrictions on access set out in the law. The implication of this definition is that, all government "computers" with vital public information are restricted from access and it is a crime to do so without authorization. A precise distinction of a private and a public computer is absent in the law.

4.2 Section 3 of the Act explains how a computer is accessed under the law making it more impractical to access information in hands of

the State. It provides that:

A person secures access to any program or data held in a computer if that person—

(a) views, alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses or destroys it; or

(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

The section is broad as it is difficult to know what kind of viewing amounts to lawful or unauthorized access. Terms like these in the law makes it difficult to those holding public information to release it and those in need of it to access it. A person standing behind an authorized person using a computer can be held liable for unauthorized access of information for viewing and is liable on conviction to imprisonment of seven years. In the same way, the person who allowed this person to view the data over his or her shoulder will be held responsible for unlawful release of information and is liable to imprisonment for ten years.

4.3 The Computer Misuse Act provides a basis of withholding information in the hands of the State and makes it difficult to access even basic information. It lacks the narrow definition of the interests of the State in protecting the citizens by setting up restrictions on access to computers with public information. It promotes secrecy other than open governance.

4.4 Section 21 (2) of the Computer Misuse Act provides that any person who attempts to commit any offence under the law commits that offence and is liable on conviction to the punishment prescribed for the offence. However, under section 22, the word attempt is defined as per section 386 of the Penal Code Act Cap 120:

(1) When a person intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

(2) It is immaterial

(a) except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention; or

(b) that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.

It is explicitly explained under the general rule of construction of the Penal Code of Uganda that the code shall be interpreted in accordance with the principles of legal interpretation obtaining in England, and expressions used in it shall be presumed, so far as is consistent with their context, and except as may be otherwise expressly provided, to be used with the meaning attaching to them in English criminal law and shall be construed in accordance therewith.

Section 387 of the Penal Code Act provides that:
Any person who attempts to commit a felony or a misdemeanour commits an offence which unless otherwise stated, is a misdemeanour. The punishment for misdemeanours under the Penal Code is a prison sentence not exceeding two years.

Since offences under the Computer Misuse Act have not explicitly been categorized as felonies or capital offences, it is unnecessary and unjust to sentence a person accused of attempting to commit an offence and a person who actually commits an offence to the same punishment.

4.5 Section 24 of the law creates an offence of cyber harassment and upon conviction, a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both. Subsection 2 further provides that for purposes of this section, cyber harassment is the use of a computer for;

(a) Making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;
(b) Threatening to inflict injury or physical harm to the person or property of any person; or
(c) Knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section

However, "obscene, lewd, lascivious or indecent behaviour" are not defined by the law, leaving the parameters so wide and prone to misinterpretation, abuse and false allegations.

4.6 Section 25 criminalizes communication that "disturb or attempts to disturb" the peace and quiet of any person with no "purpose of legitimate" communication. The section is ambiguous and creates room for misinterpretation. Sections 23 (3) and 28(5) (a) comprise broad and unclear words such as "sexually suggestive", "on reasonable grounds believes" which are not clearly defined in the law.

The short and long titles of the Act are misleading. Whereas the short title is precise, the long title is broad, confusing and unclear. It provides: An Act to make provision for safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provisions for securing the conduct of electronic transactions in a trust worthy electronic environment and to provide for other related matters.

4.7 According to the long title, the law is envisaged to regulate the safety and security of "electronic transactions and information systems". However, it does not provide a comprehensible understanding of electronic transactions and the term information systems is broadly defined as generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system. This definition gives enforcement agencies extensive powers to intervene, interfere or intercept any form of communication provided it is generated by an electronic device.

The long title further provides that the law is designed to prevent unlawful access, abuse or misuse of information systems including computers, yet "unlawful access" is not defined, rather the interpretation section defines access as gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective. The definition contains the words electronic system which is not clearly stated in the law. On the other hand, section 3 of the law as earlier discussed provides that securing access to a computer includes viewing a program or data

Plot No. 18 Stensera Road,
Block 12 Kayanja Triangle Zone Lubaga
P.O.BOX 71314
Clock Tower Kampala-Uganda
Tel: +256-414-272934, +256-414-667627
Hotline Legal +256-701-810079
Email: info@hrnjuganda.org,
humanrajournalists@yahoo.co.uk
Website: www.hrnjuganda.org
Blog: hrnjuganda.blogpost.com