ACTS
SUPPLEMENT No. 7 3rd September, 2010.

ACTS SUPPLEMENT

to The Uganda Gazette No. 53 Volume CIII dated 3rd September, 2010.

Printed by UPPC, Entebbe, by Order of the Government.

THE REGULATION OF INTERCEPTION OF COMMUNICATIONS ACT, 2010

ARRANGEMENT OF SECTIONS.

PART I—PRELIMINARY.

Section.

Section

THE REGULATION OF INTERCEPTION OF COMMUNICATIONS ACT, 2010.

An Act to provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda; to provide for the establishment of a monitoring centre; and to provide for any other related matters.

DATE OF ASSENT: 5th August, 2010.

Date of Commencement: 3rd September, 2010.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY.

1. Interpretation.

(1) In this Act, unless the context otherwise requires—

"access" means the technical ability to interface with a communications facility such as a telecommunications line or switch to enable the interception of any communication carried on that facility;

"agency" means the government telecommunications agency comprising telecommunications experts, which has been designated to operate the monitoring facility and which gives technical directions to service providers so as to ensure compliance with the provisions of this Act;

"authorised person" means a person referred to in subsection (1) of section 4;

"call" means any connection, fixed or temporary, established and transferring information between two or more users of a telecommunications system;

"call-related information" includes switching, dialing or signaling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment facility or service provided by a service provider and, where applicable, the location of the user within the telecommunications system;

"Commission" means the Uganda Communications Commission established by section 3 of the Uganda Communications Act, Cap 106;

"currency point" has the value assigned to it in the Schedule;

"customer" means—

(a) any person, body or organization which has entered into a contract with the service provider for the provision of a telecommunication service to that person, body or organization; or

(b) any person to whom or any body or organization to which a service provider provides a pre-paid telecommunication service;

"designated judge" means a judge designated by the Chief Justice to perform the functions of a designated judge for purposes of this Act;

"intercept", in relation to any communication which is sent—

(a) by means of a telecommunication system or radio communication system, means to listen to, record, read or copy the contents, whether in whole or in part;

(b) by post, means to read or copy the contents, whether in whole or in part;

"interception interface" means the physical location within the service provider's telecommunication facilities where access to the intercepted communication or call related information is provided;

"interception subject" or "interception target" means the person whose communications are to be or are being intercepted;

"key" means a numeric code or other means by which information is encrypted;

"Minister" means the Minister responsible for security or any other Minister to whom the President may from time to time assign the administration of this Act;

"monitor" includes to listen to or record a monitoring device, and "monitoring" has a corresponding meaning;

"monitoring device" means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to, read, copy or record any communication;

"monitoring centre" means a central monitoring apparatus established by section 3 (1) (a), and designated to be the monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorized person;

"national security of Uganda" includes matters relating to the existence, independence or safety of the State;

"party" in relation to a communication, means a person whose access to the communication is or might reasonably be known by all other parties;

"postal services" means the services performed and facilities provided in connection with—

(i) the collection, transmission and delivery by land, water or air of postal articles;

(ii) the issue of postage stamps and the use of franking machines;

(iii) the issue and payment of money from one place to another place or address commonly referred to as money ordering;

"protected information" means information that is encrypted by means of a key;

"relevant Ministers" means the Cabinet Ministers responsible for—

(a) defence;

(b) internal affairs; and

(c) information and communications technology;

"retention order" means an order to retain a postal article issued under section 13;

"service provider" means the provider of a postal service or telecommunication service;

"SIM-card" means the Subscriber Identity Module which is an independent, electronically activated device designed for use in conjunction with a cellular phone to enable the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to idenfify the particular Subscriber Identity Module and its installed information;

"state" means the Government of Uganda;

"telecommunication services" means a service consisting of transmission of data, voice, or images by wire, optical or other electronically guided media systems whether or not the signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other process by any means in the course of their transmission, emission or reception; and

"warrant" means an interception warrant issued under section 5.

(2) Any word or expression used in this Act, and which has been defined in the Uganda Communications Act, Cap 106, and the Uganda Posts and Telecommunications Corporation Act, Cap 107, shall have the meaning assigned to it in Uganda Communications Act and the Uganda Posts and Telecommunications Act.

PART II—CONTROL OF INTERCEPTION AND ESTABLISHMENT OF A MONITORING CENTRE.

2. Control of interception.

(1) Without prejudice to the provisions of Part VII of the Anti - Terrorism Act, Act 14 of 2002, and subject to subsection (2), no person shall—

(a) intercept any communication in the course of its transmission by means of a telecommunication system or radio communication system unless—

(i) he or she is a party to the communication;

(ii) he or she has the consent of the person to whom, or the person by whom, the communication is sent; or

(iii) he or she is authorised by warrant.

(b) intercept any communication in the course of its transmission through the post unless—

(i) he or she has the consent of the person to whom, or the person by whom, the communication is sent; or

(ii) he or she is authorised by warrant.

(2) Subsection (1) shall not apply to the bona fide interception of a communication for the purpose of or in connection with the provision, installation, maintenance or repair of a postal, telecommunication or radio communication service.

(3) Subject to subsections (1) and (2) any person who intentionally intercepts or attempts to intercept, or authorizes or procures any other person to intercept or attempt to intercept at any place, any communication in the course of its occurrence or transmission commits an offence and shall on conviction be liable to a fine not exceeding one hundred and twenty currency points or to imprisonment for a period not exceeding five years, or both.

3. Establishment of Monitoring Centre.

(1) The Minister shall, in consultation with the relevant Ministers, at the expense of the State—

(a) establish a centre to be known as the Monitoring Centre for the interception of communications under this Act;

(b) equip, operate and maintain the Monitoring Centre;

(c) acquire, install and maintain connections between telecommunication systems and the Monitoring Centre; and

(d) administer the Monitoring Centre.

(2) The Minister shall exercise responsibility over the administration and functioning of the Monitoring Centre.

(3) Notwithstanding the provisions of the Uganda Communications Act, the Monitoring Centre shall for purposes of performing its functions under this Act, be exempted from—

(a) obtaining any kind of licence required by that Act; or

(b) paying any fees payable under that Act.

(4) The Monitoring Centre shall be the sole facility through which authorised interceptions shall be effected.

(5) The Monitoring Centre shall be manned, controlled and operated by officers designated by the Minister and the relevant Ministers.

(6) The officers referred in subsection (5) shall give advice to—

(a) authorised persons; and

(b) service providers;

on the interception of communications under this Act.

PART III—APPLICATION FOR LAWFUL INTERCEPTION OF COMMUNICATIONS.

4. Authorised persons to apply for warrant of interception.

(1) An application for the lawful interception of any communication may be made by the following persons—

(a) the Chief of Defence Forces or his or her nominee;

(b) the Director General of the External Security Organisation or his or her nominee;

(c) the Director General of the Internal Security Organisation or his or her nominee; or

(d) the Inspector General of Police or his or her nominee.

(2) An application under subsection (1) shall be made by an authorised person to a designated judge to issue a warrant for the interception of any communication.

(3) An application under subsection (1) shall contain the following information—

(a) the person or customer, if known, whose communication is required to be intercepted;

(b) the service provider to whom the direction to intercept the communication must be addressed, if applicable;

(c) the nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known;

(d) full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;

(e) the period for which the warrant is required to be issued; and

(f) any other information which may be required by a designated judge to make an appropriate decision.

5. Issue of warrant.

(1) A warrant shall be issued by a designated judge to an authorised person referred to in section 4(1) 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 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.

(2) In the case of urgency or existence of exceptional circumstances, a designated judge may permit an oral application by an authorized person if the designated judge is of the opinion that it is not reasonably practicable to make a written application, but in such a case a formal application under this Part shall be lodged within forty eight hours with the designated judge.

(3) A designated judge may, if he or she is of the opinion that the circumstances so require—

(a) upon an application being made under this Part, issue an order rejecting the application; or

(b) after a warrant has been issued, amend or revoke the warrant.

6. Scope of warrant.

A warrant shall—

(a) be valid for a period of three months and may, for good cause shown by the authorised person, be renewed by a designated judge;

(b) specify the name and the address of the interception subject and the manner of interception;

(c) order the service provider to strictly comply with such technical requirements as may be specified by a designated judge to facilitate the interception;

(d) specify the apparatus and other means that are to be used for identifying the communication that is to be intercepted; and

(e) contain any other necessary details relating to the interception subject.

7. Evidence obtained in excess of a warrant.

Evidence obtained by means of an interception made in excess of a warrant issued under the provisions of this Act is admissible in evidence in criminal proceedings only with the leave of the court; and in granting or refusing such leave the court shall have regard to, among other things—

(a) the circumstances in which the evidence was obtained;

(b) the potential effect of its admission or exclusion on issues of national security; and

(c) the unfairness to the accused that may be occasioned by its admission or exclusion.

8. Assistance by service providers.

(1) A service provider shall ensure that—

(a) its postal or telecommunications systems are technically capable of supporting lawful interceptions at all times in accordance with section 11;

(b) it installs hardware and software facilities and devices to enable interception of communications at all times or when so required, as the case may be;

(c) its services are capable of rendering real time and full time monitoring facilities for the interception of communications;

(d) all call-related information is provided in real-time or as soon as possible upon call termination;

(e) it provides one or more interfaces from which the intercepted communication shall be transmitted to the monitoring centre;

(f) intercepted communications are transmitted to the monitoring centre via fixed or switched connection as may be specified by the Minister;

(g) it provides access to all the interception subjects operating temporarily or permanently within their communication systems, and, where the interception subject may be using features to divert call to other service providers or terminal equipment, access to such other providers or equipment;

(h) it provides, where necessary, the capacity to implement a number of simultaneous interceptions in order—

(i) to allow monitoring by more than one authorized person;

(ii) to safeguard the identities of monitoring agents and ensure the confidentiality of the investigations;

(i) all interceptions are implemented in such a manner that neither the interception subject nor any other unauthorized person is aware of any changes made to fulfill the warrant.

(2) Where a service provider fails to give assistance under this section—

(a) he or she commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred and twenty currency points or to imprisonment for a period not exceeding five years, or both; and

(b) the Minister responsible for Information and Communications Technology in consultation with the Uganda Communications Commission may, cancel his or her licence.

9. Duties of telecommunication service provider in relation to customer.

(1) Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, it shall obtain—

(a) the person's full name, residential address, business address, postal address and his or her identity number contained in his or her identity document, if applicable;

(b) in the case where the person is a business organization, its business name and address and the manner in which it is incorporated or registered;

(c) any other information which the telecommunication service provider deems necessary for the purpose of enabling it to comply with this Act.

(2) The telecommunication service providers shall ensure that existing subscribers register their SIM-cards within the period of six months from the date of commencement of the Act.

(3) A telecommunication service provider shall ensure that proper records are kept of the information referred to in subsection (1) and any change in such information.

10. Notice of disclosure of protected information.

(1) Subject to the provisions of this Act, where an authorised person believes on reasonable grounds—

(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.

(2) A notice under this section imposing a disclosure requirement in respect of any protected information shall—

(a) be in writing;

(b) describe the protected information to which the notice relates;

(c) specify why the protected information is required;

(d) specify a reasonable time by which a notice is to be complied with; and

(e) set out the disclosure that is required by the notice and the manner in which it is to be made.

(3) A notice under this section shall not require the making of any disclosure to any person other than—

(a) the person giving the notice; or

(b) such other person as may be identified in or under the notice.

(4) A person to whom a notice has been given under this section and who is in possession of both the protected information and the key thereto shall—

(a) use any key in his or her possession to provide access to the information;

(b) in providing such information, make a disclosure of the information in an intelligible form.

(5) Where a person to whom a notice has been given—

(a) has been in possession of any key to the protected information, but no longer possesses it; and

(b) has information that will facilitate the obtaining or discovery of the key to protected information;

he or she shall disclose the information referred to in paragraph (b) to the authorised person.

(6) A person who fails to make the disclosure required by a notice issued under this section commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred and twenty currency points or to imprisonment for a period not exceeding five years, or both.

11. Interception capability of telecommunication service.

(1) Notwithstanding any other law, a telecommunication service provider shall—

(a) provide a telecommunication service which has the capability to be intercepted; and

(b) store call-related information in accordance with a directive issued under subsection (2).

(2) The Minister responsible for Information and Communications Technology shall, on the commencement of this Act, issue a directive to telecommunication service providers specifying—

(a) the manner in which effect is to be given to subsection (1) by every telecommunication service provider; and

(b) the security, technical and functional requirements of the facilities and devices to be acquired by every telecommunication service provider to enable—

(i) the interception of communication under this Act; and

(ii) the storing of call-related information; and

(c) the period within which the directive must be complied with.

(3) A directive referred to in subsection (2) shall specify—

(a) the capacity and technical features of the devices or systems to be used for interception purposes;

(b) the connectivity of the devices or systems to be used for interception purposes with the monitoring centre;

(c) the manner of routing intercepted information to the monitoring centre; and

(d) any other relevant matter which the Minister responsible for Information and Communications Technology deems necessary or expedient.

(4) Notwithstanding any other law, agreement or licence, a telecommunication service provider shall, at its own expense, acquire whether by purchasing or leasing, the facilities and devices specified in a directive issued under subsection (2).

(5) Subject to section 12, any cost incurred by a telecommunication service provider under this Act for the purpose of—

(a) enabling—

(i) a telecommunication service to be intercepted; and

(ii) call-related information to be stored; and

(b) complying with this section and section 8;

shall be borne by the telecommunication service provider.

(6) A directive issued under sub-section (2) may in a like manner be amended or withdrawn.

12. Compensation payable to service provider or protected information key holder.

(1) The Minister shall, after consultation with the Minister responsible for Information and Communications Technology, by Notice in the *Gazette* prescribe—

(a) the nature or form of assistance given by a service provider or protected information key holder in the execution of a warrant or directive issued under this Act for which it must be compensated by the State; and

(b) reasonable tariffs of compensation payable to a service provider or protected information key holder for providing the nature or form of the assistance referred to in paragraph (a).

(2) The tariffs prescribed under paragraph (b) of subsection (1)—

(a) may differ in respect of different categories of service providers or protected information key holders;

(b) shall be uniform in respect of each service provider or protected information key holder falling within the same category.

(3) The nature or form of assistance referred to in paragraph (a) of subsection (1) shall include, in the case of—

(a) a telecommunication service provider, the making available of a facility, device or telecommunication system;

(b) a protected information key holder—

(i) the disclosure of the key; and

(ii) the provision of assistance in rendering intelligible the protected information.

(4) The compensation payable to a service provider or protected information key holder shall only be for direct costs incurred in respect of personnel and administration services which are required for purposes of providing any of the forms of assistance referred to in paragraph (a) of subsection (1).

PART IV—POSTAL ARTICLES

13. Application for a retention order.

(1) Where an authorised person suspects on reasonable grounds that a postal article in the custody of a postal service provider—

(a) contains anything in respect of which an offence or attempted offence is being committed; or

(b) contains anything that will afford evidence of the commission of an offence; or

(c) is being sent to further the commission of an offence;

(d) needs to be obtained and examined in the interests of defence, public safety or public order;

he or she may apply to a designated judge for a retention order to retain the postal article for the purpose of examination.

(2) Where a designated judge, by written order to the authorized person and the postal service provider, certifies that it is necessary for any of the purposes specified in paragraphs (a), (b), (c) or (d) of section (1) to order that a postal article in the postal service provider's custody should be retained and, if so required by the order, opened and examined, the postal service provider shall forthwith retain the postal article.

(3) Section 4 shall apply with such modifications as may be necessary to the information required to be furnished to a designated judge before a retention order is issued.

14. Examination and accountability for retained postal article.

(1) On the day appointed by or under a retention order, the authorised person shall, in the presence of a representative of the postal service provider, examine the retained postal article.

(2) Where, on examination of a postal article under subsection (1), the suspicion that gave rise to its examination—

(a) is substantiated, the postal article may be retained for the purposes of evidence in a criminal prosecution or destroyed or dealt with in such other manner as may be authorized by the retention order;

(b) is not substantiated, the postal article shall be delivered to the person to whom it is addressed or to his or her representative on payment of the postage payable on the article.

PART V—GENERAL

15. Restriction on disclosure.

(1) No person may disclose any communication or information which he or she obtained in the exercise of his or her powers or the performance of his or her duties under this Act, except—