SPECIAL ISSUE

Kenya Gazette Supplement No. 91 (National Assembly Bills No. 29)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

NATIONAL ASSEMBLY BILLS, 2017

NAIROBI, 13th June, 2017

CONTENT

Bill for Introduction into the National Assembly —

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

THE COMPUTER AND CYBERCRIMES BILL, 2017

ARRANGEMENT OF CLAUSES

Clause

PART III—INVESTIGATION PROCEDURES

PART IV— INTERNATIONAL COOPERATION

PART V—GENERAL PROVISIONS

THE COMPUTER AND CYBERCRIMES BILL, 2017

A Bill for

AN ACT of Parliament to provide for offences relating to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes

ENACTED by the Parliament of Kenya as follows—

PART 1—PRELIMINARY

Short title.

1. This Act may be cited as the Computer and Cybercrimes Act, 2017.

Interpretation.

2. In this Act, unless the context otherwise requires—

"access" means gaining entry into or intent to gain entry by a person to a program or data stored in a computer system and the person either—

(a) alters, modifies or erases a program or data or any aspect related to the program or data in the computer system;

(b) copies, transfers or moves a program or data to—

(i) any computer system, device or storage medium other than that in which it is stored; or

(ii) to a different location in the same computer system, device or storage medium in which it is stored;

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

(d) uses it by causing the computer to execute a program or is itself a function of the program;

"Authority" has the meaning assigned to it under section 3 of the Kenya Information Communications Act; Cap 411A.

"authorised person" means a person designated by the Cabinet Secretary by notice in the Gazette for the purposes of Part III of this Act;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters relating to Information, Communications and Technology;

"Central Authority" has the same meaning assigned to it under section 2 of the Mutual Legal Assistance Act, 2011; No. 36 of 2011.

"computer data storage medium" means a device, whether physical or virtual, containing or designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed form for use by a computer, and from which data is capable of being reproduced;

"computer system" means a physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system;

"content data" means the substance, its meaning or purport of a specified communication;

"data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"interception" means the monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system over a telecommunications system, and includes, in relation to a function of a computer system, listening to or recording a function of a computer system or acquiring the substance, its meaning or purport of such function;

"interference" means any impairment to the confidentiality, integrity or availability of a computer system, or any program or data on a computer system, or any act in relation to the computer system which impairs the operation of the computer system, program or data;

"premises" includes land, buildings, movable structures, vehicles, vessels or aircraft;

"program" means data representing instructions or statements that, if executed in a computer system, causes the computer system to perform a function and reference to a program includes a reference to a part of a program;

"requested State" has the meaning assigned to it under section 2 of the Mutual Legal Assistance Act, 2011; No. 36 of 2011.

"requesting State" has the meaning assigned to it under section 2 of the Mutual Legal Assistance Act, 2011; No. 36 of 2011.

"seize" with respect to a program or data includes to—

(a) secure a computer system or part of it or a device;

(b) make and retain a digital image or secure a copy of any program or data, including using an on-site equipment;

(c) render the computer system inaccessible;

(d) remove data in the accessed computer system; or

(e) obtain output of data from a computer system;

"service provider" means—

(a) a public or private entity that provides to users of its services the means to communicate by use of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established—

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal, geographic location, electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the

installation of telecommunication apparatus, available on the basis of the service agreement or arrangement;

"telecommunication apparatus" means an apparatus constructed or adapted for use in transmitting anything which is transmissible by a telecommunication system or in conveying anything which is transmitted through such a system;

"telecommunication system" means a system for the conveyance, through the use of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of—

(a) speech, music or other sounds;

(b) visual images;

(c) data;

(d) signals serving for the impartation, whether as between persons and persons, things and things or persons and things, of any matter otherwise than in the form of sound, visual images or data; or

(e) signals serving for the activation or control of machinery or apparatus and includes any cable for the distribution of anything falling within paragraphs (a), (b),(c) or (d);

"traffic data" means computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or the type of underlying service.

Objects of the Act.

3. The objects of this Act are to—

(a) protect the confidentiality, integrity and availability of computer systems, programs and data;

(b) prevent the unlawful use of computer systems;

(c) facilitate the investigation and prosecution of cybercrimes; and

(d) facilitate international co-operation on matters

covered under this Act.

PART II—OFFENCES

Unauthorised access.

4. (1) A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

(2) Access by a person to a computer system is unauthorised if—

(a) that person is not entitled to control access of the kind in question to the program or data; or

(b) that person does not have consent from any person who is entitled to access the computer system through any function to the program or data.

(3) For the purposes of this section, it is immaterial that the unauthorised access is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

Access with intent to commit further offence.

5. (1) A person who commits an offence under section 4 with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person, commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.

(2) For the purposes of this subsection (1), it is immaterial that the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorised interference.

6. (1) A person who intentionally and without authorisation does any act which causes an unauthorised interference, to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a

term not exceeding five years, or to both.

(2) For the purposes of this section, an interference is unauthorised, if the person whose act causes the interference—

(a) is not entitled to cause that interference;

(b) does not have consent to interfere from a person who is so entitled.

(3) A person who commits an offence under subsection (1) which,—

(a) results in a significant financial loss to any person;

(b) threatens national security;

(c) causes physical injury or death to any person; or

(d) threatens public health or public safety,

is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(4) For the purposes of this section, it is immaterial whether or not the unauthorised interference is directed at—

(a) any particular computer system, program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(5) For the purposes of this section, it is immaterial whether an unauthorised modification or any intended effect of it is permanent or temporary.

Unauthorised interception.

7. (1) A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(2) A person who commits an offence under subsection (1) which—

(a) results in a significant financial loss;

(b) threatens national security;

(c) causes physical injury or death to any person; or

(d) threatens public health or public safety,

is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term of not exceeding ten years, or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised interception is not directed at —

(a) a telecommunication system;

(b) any particular computer system data;

(c) a program or data of any kind; or

(d) a program or data held in any particular computer system.

(4) For the purposes of this section, it is immaterial whether an unauthorised interception or any intended effect of it is permanent or temporary.

Illegal devices and access codes.

8. (1) A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(2) A person who knowingly receives, or is in possession of, a program or a computer password, device, access code, or similar data from any action specified under subsection (1) and intends that it be used to commit or assist in commission of an offence under this Part, without sufficient excuse or justification, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(3) Despite subsections (1) and (2), the activities described in thereof do not constitute an offence if —

(a) any act intended for the authorised training, testing or protection of a computer system; or

(b) the use of a program or a computer password, access code, or similar data is undertaken in compliance of and in accordance with the terms of a judicial order issued or in exercise of any power under this Act or any law.

(4) For the purposes of subsections (1) and (2), possession of any program or a computer password, access code, or similar data includes having—

(a) possession of a computer system which contains the program or a computer password, access code, or similar data;

(b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or

(c) control of a program or a computer password, access code, or similar data that is in the possession of another person.

Unauthorised disclosure of password or access code.

9. (1) A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment term for a term not exceeding three years, or to both.

(2) A person who commits the offence under subsection (1)—

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) to occasion any loss,

is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

Enhanced penalty for offences involving protected computer system.

10. (1) Where a person commits any of the offences specified under sections 4, 5, 6 and 7 on a protected computer system, that person shall be liable, on conviction, to a fine not exceeding twenty five million shillings or imprisonment term not exceeding twenty years or both.

(2) For purposes of this section—

"protected computer system" means a computer

system used directly in connection with, or necessary for, —

(a) the security, defence or international relations of Kenya;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically;

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services;

(e) the provision of national registration systems; or

(f) such other systems as may be designated by the Cabinet Secretary in the manner or form as the Cabinet Secretary may consider appropriate.

Cyber espionage.

11. (1) A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to—

(a) gain access, as provided under section 4, to critical data, a critical database or a national critical information infrastructure; or

(b) intercept data , as provided under section 7, to, from or within a critical database or a national critical information infrastructure, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya,

commits an offence and is liable, on conviction, to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.

(2) A person who unlawfully and intentionally possesses, communicates, delivers or makes available or receives, data , to, from or within a critical database or a national critical information infrastructure, with the intention to directly or indirectly benefit a foreign state

against the Republic of Kenya, commits an offence and is liable on conviction to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.

(3) A person who unlawfully and intentionally performs or authorizes, or allows another person to perform a prohibited act as envisaged under this Act in order to gain access, as provided under section 4 ,to or intercept data ,as provided under section 7, which is in possession of the State and which is exempt information in accordance with the law relating to access to information, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya , commits an offence and is liable , on conviction, to a fine not exceeding five million or to imprisonment for a period not exceeding ten years or to a fine not exceeding five million , or to both.

False publications.

12. A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

Child pornography.

13. (1) A person who, intentionally—

(a) publishes child pornography through a computer system;

(b) produces child pornography for the purpose of its publication through a computer system; or

(c) possesses child pornography in a computer system or on a computer data storage medium,

commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty five years, or to both.

(2) It is a defence to a charge of an offence under subsection (1) (a) or (c) if the person establishes that the child pornography was intended for a bona fide scientific, research, medical or law enforcement purpose.

(3) For purposes of this section—

"child" means a person under the age of eighteen years;

"child pornography" includes data which, whether

visual or audio, depicts—

(a) a child engaged in sexually explicit conduct;

(b) a person who appears to be a child engaged in sexually explicit conduct; or

(c) realistic images representing a child engaged in sexually explicit conduct;

"publish" includes to—

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(b) having in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature for the purpose of doing an act referred to in paragraph (a).

Computer forgery.

14. (1) A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(2) A person who commits an offence under subsection (1), dishonestly or with similar intent—

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any economic benefit for oneself or for another person,

is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

Computer fFraud.

15. (1) A person who, with fraudulent or dishonest intent —

(a) unlawfully gains;

(b) occasions unlawful loss to another person; or

(c) obtains an economic benefit for oneself or for another person,

through any of the means described in subsection (2), commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both.

(2) For purposes of subsection (1) the word " means" refers to —

(a) an unauthorised access to a computer system , program or data;

(b) any input, alteration, modification, deletion, suppression or generation of any program or data;

(c) any interference, hindrance, impairment or obstruction with the functioning of a computer system;

(d) copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; or

(e) uses any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner.

Cyberstalking and cyber-bullying.

16. (1) A person who, individually or with other persons, wilfully and repeatedly communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—

(a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or

(b) detrimentally affects that person.

(2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not

exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(3) It is a defence to a charge of an offence under this section if the person establishes that—

(a) the conduct was pursued for the purpose of preventing or detecting crime;

(b) the conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under the enactment; or

(c) in the particular circumstances, the conduct was in the public interest.

Aiding or abetting in the commission of an offence.

17. (1) A person who knowingly and willfully aides or abets the commission of any offence under this Act commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.

(2) A person who knowingly and willfully attempts to commit an offence or does any act preparatory to or in furtherance of the commission of any offence under this Act, commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.

Offences by a body corporate and limitation of liability.

18. (1) Where any offence under this Act has been committed by a body corporate—

(a) the body corporate is liable, on conviction, to a fine not exceeding fifty million shillings; and

(b) every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity, is also deemed to have committed the offence, unless they prove the offence was committed without their consent or knowledge and that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their functions and to prevailing circumstances, and is liable, on conviction, to a fine not exceeding five million shillings or imprisonment for a term not

exceeding three years, or to both .

(2) If the affairs of the body corporate are managed by its members, subsection (1) (b) applies in relation to the acts or defaults of a member in connection with their management functions, as if the member was a principal officer of the body corporate or was acting in a similar capacity.

Confiscation or forfeiture of assets.

19. (1) A court may order the confiscation or forfeiture of monies, proceeds, properties and assets purchased or obtained by a person with proceeds derived from or in the commission of an offence under this Act.

(2) The court may, on conviction of a person for any offence under this Act make an order of restitution of any asset gained from the commission of the offence, in accordance with the provisions and procedures of the Proceeds of Crime and Anti-Money Laundering Act, 2009. No. 9 of 2009.

Compensation oOrder.

20. (1) Where the court convicts a person for any offence under this Part, or for an offence under any other law committed through the use of a computer system, the court may make an order for the payment by that person of a sum to be fixed by the court as compensation to any person for any resultant loss caused by the commission of the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of any offence committed under this Part is deemed to have been satisfied to the extent of any amount which they have been paid under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order of compensation under this section is recoverable as a civil debt.

Offences committed through the use of a computer system.

21. A person who commits an offence under any other law, through the use of a computer system, is liable on conviction, in addition to the penalty provided under that law to a fine not exceeding three million shillings or to imprisonment term for a term not exceeding four years, or to both.

PART III—INVESTIGATION PROCEDURES

Scope of procedural

22. (1) All powers and procedures under this Act are

applicable to and may be exercised with respect to any— provisions.

(a) criminal offences provided under this Act;

(b) other criminal offences committed by means of a computer system established under any other law; and

(c) the collection of evidence in electronic form of a criminal offence under this Act or any other law.

(2) In any proceedings related to any offence, under any law of Kenya, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted.

(3) The powers and procedures provided under this Part are without prejudice to the powers granted under—

(a) the National Intelligence Service Act, 2012; No.28 of 2012.

(b) the National Police Service Act, 2011; No. 30 of 2011.

(c) the Kenya Defence Forces Act, 2012; and No. 25 of 2012.

(d) any other relevant law.

Search and seizure of stored computer data.

23. (1) Where a police officer or an authorised person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data, that—

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or

(b) has been acquired by a person as a result of the commission of an offence,

the police officer or the authorised person may apply to the court for issue of a warrant to enter any premises to access, search and similarly seize such data.

(2) When making an application under subsection (1), the police officer or the authorised person shall—

(a) explain the reason they believe that the material sought may be found on the premises to be searched;

(b) state that the search may be frustrated or seriously prejudiced unless an investigating officer may at the first instance on arrival at the premises secure immediate entry to the premises;

(c) identify and explain, the type of evidence

suspected to be found on the premises; and

(d) explain the measures that shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as imaging, mirroring or copying of relevant data and not through physical custody of computer system, program, data, or computer data storage medium.

(3) Where the court is satisfied by the explanations provided under subsection (2), the court shall issue a warrant authorising a police officer or an authorised person to—

(a) access, seize or secure the specified computer system, program, data or computer data storage medium;

(b) access, inspect and check the operation of any computer system to which the warrant issued under this section applies;

(c) access any information, code or technology which is capable of unscrambling encrypted data contained or available to such computer system into an intelligible format for the purpose of the warrant issued under this section;

(d) require any person possessing knowledge concerning the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary computer data or information, to enable the police officer or any authorised person in conducting such activities as authorised under this section;

(e) require any person in possession of decryption information to grant them access to such decryption information necessary to decrypt data required for the purpose of the warrant issued under this section , except where such decryption may contravene the protection of such person against self-incrimination under the laws of Kenya;

(f) require any person possessing appropriate technical knowledge to provide such reasonable

technical and other assistance as they may require for the purposes of executing the warrant issued under this section.

(4) Where a police officer or an authorised person is authorised to search or access a specific computer system or part of it, under subsection (3), and has reasonable grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is accessible from or available to the initial system, the police officer or the authorised person may extend the search or access to such other systems or systems.

(5) The computer data seized pursuant to the provisions of this section may be used only for the purpose of which it was originally obtained.

(6) A warrant issued under this section shall only be used for the purpose for which it was originally obtained.

(7) The police officer or authorised person shall—

(a) seize a computer system under subsection (1) only if—

(i) it is not practical to seize or similarly secure the computer data; or

(ii) it is necessary to ensure that data shall not be destroyed, altered or otherwise interfered with; and; and

(b) exercise reasonable care, where the computer system or computer data storage medium is retained.

(8) A person who—

(a) obstructs the lawful exercise of the powers under this section; or

(b) misuses the powers granted under this section,commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment for term not exceeding three years, or to both.

(9) For purposes of this section—

"decryption information" means information or technology that enables a person to readily unscramble encrypted data into an intelligible format;

"encrypted data" means data which has been transformed from its plain text version to an unintelligible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; and

"plain text version" means original data before it has been transformed into an unintelligible format.

Power to search without a warrant in special circumstances.

24. (1) Subject to section 23, a police officer may, in special circumstances enter, without a warrant any premises in or on which the police officer suspects an offence under this Act has been or is likely to be committed, and take possession of such computer system.

Cap 75.

(2) Sections 119, 120 and 121 of the Criminal Procedure Code relating to execution of search warrant, and the provisions of that code as to searches apply to a search without warrant under this section.

(3) For purposes of conducting a search under this section, the police officer shall carry with them, and produce to the occupier of the premises on request by that occupier, the police officer's certificate of appointment.

(4) Where anything is seized under subsection (1), the police officer shall immediately make a record describing anything that has been seized, and without undue delay take or cause it to be taken before a court within whose jurisdiction the thing was found, to be dealt with according to the law.

Record of and access to seized data.

25. (1) Where a computer system or data has been removed or rendered inaccessible, following a search or a seizure under section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search—

(a) make a list of what has been seized or rendered inaccessible, and shall specify the date and time of seizure; and

(b) provide a copy of the list to the occupier of the premises or the person in control of the computer system referred to under paragraph (a).

(2) Subject to subsection (3), a police officer or an

authorised person shall, on request, permit a person who—

(a) had the custody or control of the computer system;

(b) has a right to any data or information seized or secured; or

(c) has been acting on behalf of a person under subsection (1)(a) or (b),

to access and copy computer data on the system or give the person a copy of the computer data.

(3) The police officer or authorised person may refuse to give access or provide copies under subsection (2), if they have reasonable grounds for believing that giving the access or providing the copies, may—

(a) constitute a criminal offence; or

(b) prejudice—

(i) the investigation in connection with the search that was carried out;

(ii) an ongoing investigation; or

(iii) any criminal proceeding that is pending or that may be brought in relation to any of those investigations.

(4) Despite subsection (3), a court may, on reasonable grounds being disclosed, allow a person who has qualified under subsection (2) (a) or (b) —

(a) access and copy computer data on the system; or

(b) obtain a copy of the computer data.

Production order.

26. (1) Where a police officer or an authorised person has reasonable grounds to believe that—

(a) specified data stored in a computer system or a computer data storage medium is in the possession or control of a person in its territory; and

(b) specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the

purposes of the investigation,

the police officer or the authorised person may apply to court for an order requiring—

(i) such person in its territory to submit specified computer data that is in that person's possession or control, and is stored in a computer system or a computer data storage medium; or

(ii) such a service provider offering its services in Kenya to submit subscriber information relating to such services in that service provider's possession or control.

(2) When making an application under subsection (1), the police officer or an authorised person shall—

(a) explain the reasons they believe that the specified computer data sought is likely to be in the possession of the persons mentioned in subsection (1) (a) and (b);

(b) state whether the purpose of the investigation may be frustrated or seriously prejudiced, if the specified computer data or the subscriber information, as the case may be, is not produced;

(c) identify and explain the type of evidence that is likely suspected to be produced by the persons mentioned in subsections (1) (a) and (b);

(d) identify and explain the subscribers, users or unique identifiers which are the subject of an investigation or prosecution which he believes that it may be disclosed as a result of the production of the specified computer data;

(e) identify and explain, the identified offence, in respect of which the production order is sought;

(f) specify the measures to be taken to prepare and ensure that the specified computer data shall be produced—

(i) while maintaining the privacy of other users, customers and third parties; and

(ii) without disclosing data of any party who is not part of the investigation; and

(iii) and measures to be taken to prepare and ensure that the production of the specified

computer data is carried out through a technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.

(3) Where the court is satisfied with the explanations provided under subsection (2), the court shall issue the order applied for under subsection (1).

(4) The court may also require that the recipient of the order as well as any person in control of the computer system keep confidential the existence of the warrant and exercise of power under this section.

(5) A person who fails to comply with an order under this section or misuses the powers granted under this section commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a period not exceeding three years, or to both.

(6) Despite the provisions of this section, upon an application in writing by a police officer that demonstrates to the satisfaction of the designated Office of the Inspector-General of Police that there exist reasonable grounds to believe that specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control which is necessary or desirable for the purposes of any investigation, the designated Office may order such a service provider to submit subscriber information relating to such services in that service provider's possession or control.

Expedited preservation and partial disclosure of traffic data.

27. (1) Where a police officer or an authorised person has reasonable grounds to believe that—

(a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible,

the police officer or an authorised person shall serve a

notice on the person who is in possession or control of the computer system, requiring the person to—

(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or

(ii) disclose sufficient traffic data concerning any communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice shall be preserved and its integrity shall be maintained for a period not exceeding the period specified in the notice.

(3) The period of preservation and maintenance of integrity may be extended for a period exceeding thirty days if, on an application by the police officer or authorised person, the court is satisfied that—

(a) an extension of preservation is reasonably required for the purposes of an investigation or prosecution;

(b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible; and

(c) the cost of the preservation is not overly burdensome on the person in control of the computer system.

(4) The person in receipt of the order as well as any person in control of the computer system shall keep confidential the existence of the order and exercise of power under this section.

(5)The person in possession or control of the computer system shall be responsible to preserve the data specified—

(a) for the period of notice for preservation and maintenance of integrity or for any extension thereof permitted by the court; and

(b) for the period of the preservation to keep confidential any preservation ordered under this section.

(6) Where the person in possession or control of the computer system is a service provider, the service provider

shall be required to—

(a) respond expeditiously to a request for assistance, whether to facilitate requests for police assistance, or mutual assistance requests; and

(b) disclose as soon as practicable, a sufficient amount of the non-content data to enable a police officer or an authorised person to identify any other telecommunications providers involved in the transmission of the communication.

(7) The powers of the police officer or an authorised person under subsection (1) shall apply whether there is one or more service providers involved in the transmission of communication which is subject to exercise of powers under this section.

Real-time collection of traffic data.

28. (1) Where a police officer or an authorised person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a specific criminal investigation, the police officer or authorised person may apply to the court for an order to—

(a) permit the police officer or authorised person to collect or record through the application of technical means traffic data, in real-time;

(b) compel a service provider, within its existing technical capability—

(i) to collect or record through application of technical means traffic data in real time; or

(ii) to cooperate and assist a police officer or an authorised person in the collection or recording of traffic data, in real-time, associated with specified communications in its jurisdiction transmitted by means of a computer system.

(2) In making an application under subsection (1), the police officer or an authorised person shall—

(a) state the grounds they believe the traffic data sought is available with the person in control of the computer system;

(b) identify and explain, the type of traffic data

suspected to be found on such computer system;

(c) identify and explain the subscribers, users or unique identifier the subject of an investigation or prosecution suspected as may be found on such computer system;

(d) identify and explain the offences identified in respect of which the warrant is sought; and

(e) explain the measures to be taken to prepare and ensure that the traffic data shall be sought—

(i) while maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data to any party not part of the investigation.

(3) Where the court is satisfied with the explanations provided under subsection (2), the court shall issue the order provided for under subsection (1).

(4) For purposes of subsection (1), real-time collection or recording of traffic data shall not be ordered for a period not exceeding six months.

(5) The court may authorize an extension of time under subsection (4), if it is satisfied that—

(a) such extension of real-time collection or recording of traffic data is reasonably required for the purposes of an investigation or prosecution;

(b) the extent of real-time collection or recording of traffic data is commensurate, proportionate and necessary for the purposes of investigation or prosecution;

(c) despite prior authorisation for real-time collection or recording of traffic data, additional real-time collection or recording of traffic data is necessary and needed to achieve the purpose for which the warrant is to be issued;

(d) measures taken to prepare and ensure that the real-time collection or recording of traffic data is carried out while maintaining the privacy of other users, customers and third parties and without the

disclosure of information and data of any party not part of the investigation;

(e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of traffic data is permitted; and

(f) the cost of such preservation is not overly burdensome upon the person in control of the computer system.

(6) A court may, in addition to the requirement specified under subsection (3) require the service provider to keep confidential the order and execution of any power provided under this section.

(7) A service provider who fails to comply with an order under this section commits an offence and is liable on conviction—

(a) where the service provider is a corporation, to a fine not exceeding ten million; or

(b) in case of a principal officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

Interception of content data.

29. (1) Where a police officer or an authorised person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for the purposes of a specific investigation in respect of a serious offence, the police officer or authorised person may apply to the court for an order to—

(a) permit the police officer or authorised person to collect or record through the application of technical means;

(b) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications within the jurisdiction transmitted by

means of a computer system.

(2) In making an application under subsection (1), the police officer or an authorised person shall—

(a) state the reasons he believes the content data being sought is in possession of the person in control of the computer system;

(b) identify and state the type of content data suspected to be found on such computer system;

(c) identify and state the offence in respect of which the warrant is sought;

(d) state if they have authority to seek real-time collection or recording on more than one occasion is needed, and shall specify the additional number of disclosures needed to achieve the purpose for which the warrant is to be issued;

(e) explain measures to be taken to prepare and ensure that the real-time collection or recording is carried out—

(i) while maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of information and data of any party not part of the investigation;

(f) state how the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) state the manner in which they shall achieve the objective of the warrant, real time collection or recording by the person in control of the computer system where necessary.

(3) Where the court is satisfied with the grounds provided under subsection (2), the court shall issue the order applied for under subsection (1).

(4) For purposes of subsection (1), the real-time collection or recording of content data shall not be ordered for a period that exceeds the period that is necessary for the collection thereof and in any event not for more than a period of nine months.

(5) The period of real-time collection or recording of

content data may be extended for such period as the court may consider necessary where the court is satisfied that—

(a) such extension of real-time collection or recording of content data is required for the purposes of an investigation or prosecution;

(b) the extent of real-time collection or recording of content data is proportionate and necessary for the purposes of investigation or prosecution;

(c) despite prior authorisation for real-time collection or recording of content data, further real-time collection or recording of content data is necessary to achieve the purpose for which the warrant is to be issued;

(d) measures shall be taken to prepare and ensure that the real-time collection or recording of content data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;

(e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of content data is permitted; and

(f) the cost of such real-time recording and collection is not overly burdensome upon the person in control of the computer system.

(6) The court may also require the service provider to keep confidential the order and execution of any power provided for under this section.

(7) A service provider who fails to comply with an order under this section commits an offence and is liable, on conviction—

(a) where the service provider is a corporation, to a fine not exceeding ten million;

(b) in case of an officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

Obstruction and misuse.

30. (1) A person who obstructs the lawful exercise of the powers under this Part, including destruction of data, or

fails to comply with the requirements of this Part is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

(2) A police officer or an authorised person who misuses the exercise of powers under this Part commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

Appeal.

31. Any person aggrieved by any decision or order of the Court made under this Part, may appeal to the High Court or Court of Appeal as the case may be within thirty days from the date of the decision or order.

Confidentiality and limitation of liability.

32. (1) A service provider shall not be subject to any civil or criminal liability, unless it is established that the service provider had actual notice, actual knowledge, or willful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by a service provider in connection with a contravention of this Act or any other written law.

(2) A service provider shall not be liable under this Act or any other law for maintaining and making available the provision of their service.

(3) A service provider shall not be liable under this Act or any other law for the disclosure of any data or other information that the service provider discloses only to the extent required under this Act or in compliance with the exercise of powers under this Part.

PART IV—INTERNATIONAL COOPERATION

General principles relating to international co-operation. No. 36 of 2011.

33. (1) This Part shall apply in addition to the Mutual Legal Assistance Act, 2011.

(2) The Central Authority may make a request for mutual legal assistance in any criminal matter to a requested State for purposes of—

(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or data;

(b) collecting evidence of an offence in electronic form; or

(c) obtaining expeditious preservation and disclosure of traffic data, real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act. No. 36 of 2011.

(3) A requesting State may make a request for mutual legal assistance to the Central Authority in any criminal matter, for the purposes provided in subsection (2).

(4) Where a request has been received under subsection (3), the Central Authority may, subject to the provisions of the Mutual Legal Assistance Act, 2011, this Act and any other relevant law—

(a) grant the legal assistance requested; or

(b) refuse to grant the legal assistance requested.

(5) The Central Authority may require a requested State to—

(a) keep the contents, any information and material provided in a confidential manner;

(b) only use the contents, information and material provided for the purpose of the criminal matter specified in the request; and

(c) use it subject to other specified conditions.

Spontaneous information.

34. (1) The Central Authority may, subject to this Act and any other relevant law, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences or might lead to a request for co-operation by the foreign State under this Act.

(2) Prior to providing the information under subsection (1), the Central Authority may request that such information be kept confidential or only subject to other specified conditions.

(3) Where a foreign State cannot comply with the specified conditions specified under subsection (2), the State shall notify the Central Authority as soon as practicable.

(4) Upon receipt of a notice under subsection (3), the Central Authority may determine whether to provide such information or not.

(5) Where the foreign State accepts the information subject to the conditions specified by the Central Authority, that State shall be bound by them.

Expedited preservation of stored computer data.

35. (1) Subject to section 33, a requesting State which has the intention to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of data, may request the Central Authority to obtain the expeditious preservation of data stored by means of a computer system, located within the territory of Kenya.

(2) When making a request under subsection (1), the requesting State shall specify—

(a) the authority seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored computer data to be preserved and its connection to the offence;

(d) any available information identifying the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored computer data.

(3) Upon receiving the request under this section, the Central Authority shall take the appropriate measures to preserve the specified data in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) A preservation of stored computer data effected under this section, shall be for a period of not less one hundred and twenty days, in order to enable the requesting State to submit a request for the search or access, seizure or securing, or the disclosure of the data.

(5) Upon receipt for a request under this section, the data shall continue to be preserved pending the final decision being made with regard to that request.

Expedited disclosure of preserved traffic data.

36. Where during the course of executing a request under section 33 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Central Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

Mutual assistance regarding accessing of stored computer data.

37. (1) Subject to section 33, a requesting State may request the Central Authority to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of Kenya, including data that has been preserved in accordance with section 36.

(2) When making a request under subsection (1), the requesting State shall—

(a) give the name of the authority conducting the investigation or proceedings to which the request relates;

(b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws;

(c) give a description of the purpose of the request and of the nature of the assistance being sought;

(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested State, give details of the offence in question, particulars of the investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;

(e) give details of any procedure that the requesting State wishes to be followed by the requested State in giving effect to the request, particularly in the case of a request to take evidence;

(f) include a statement setting out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes;

(g) give details of the period within which the requesting State wishes the request to be complied with;

(h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the requested State;

(i) give details of the stored computer data, data or program to be seized and its relationship to the offence;

(j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or electronic device;

(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and

(l) give any other information that may assist in giving effect to the request.

(3) Upon receiving the request under this section, the Central Authority shall take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation in accordance with subsection (3), including any warrants to execute the request, the Central Authority may seek the support and cooperation of the requesting State during such search and seizure.

(5) Upon conducting the search and seizure request, the Central Authority shall, subject to section 33, provide the results of the search and seizure as well as electronic or physical evidence seized to the requesting State.

Trans-border access to stored computer data with consent or where publicly available.

38. A police officer or another authorised person may, without the authorisation but subject to any applicable provisions of this Act—

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in its territoryKenya, stored computer data located in another territory, if such police officer or another authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.

Mutual assistance in the real-time collection of traffic data.

39. (1) Subject to Section 33, a requesting State may request the Central Authority to provide assistance in real-time collection of traffic data associated with specified communications in Kenya transmitted by means of a computer system.

(2) When making a request under subsection (1), the requesting State shall specify—

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority with access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose for the required traffic data;

(f) sufficient information to identify the traffic data;

(g) any further details relevant traffic data;

(h) the necessity for use of powers under this section; and

(i) the terms for the use and disclosure of the traffic data to third parties.

(3) Upon receiving the request under this section, the Central Authority shall take all appropriate measures to

obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the search and seizure.

(5) Upon conducting the measures under this section the Central Authority shall, subject to section 33, provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the requesting State.

Mutual assistance regarding the interception of content data.

40. (1) Subject to section 33, a requesting State may request the Central Authority to provide assistance in the real-time collection or recording of content data of specified communications in the territory of Kenya transmitted by means of a computer system.

(2) When making a request under subsection (1), a requesting State shall specify—

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority with access to the relevant communication;

(d) the location at which or nature of the communication;

(e) the intended purpose for the required communication;

(f) sufficient information to identify the communications;

(g) details of the data of the relevant interception;

(h) the recipient of the communication;

(i) the intended duration for the use of the communication;

(j) the necessity for use of powers under this section; and

(k) the terms for the use and disclosure of the communication to third parties.

(3) Upon receiving the request under this section, the Central Authority shall, take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation, including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the search and seizure.

(5) Upon conducting the measures under this section the Central Authority shall subject to section 33, provide the results of such measures as well as real-time collection or recording of content data of specified communications to the requesting State.

Point of contact.

41. (1) The Central Authority shall ensure that the, investigation agency responsible for investigating and prosecuting cybercrime, shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, including carrying out the following measures—

(a) the provision of technical advice;

(b) the preservation of data pursuant to sections 35 and 36;

(c) the collection of evidence, the provision of legal information, and locating of suspects,

within expeditious timelines to be defined by regulations under this Act.

(2) The point of contact shall be resourced with and possess the requisite capacity to securely and efficiently

carry out communications with other points of contact in other territories, on an expedited basis.

(3) The point of contact shall have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act.

PART V—GENERAL PROVISIONS

Territorial jurisdiction.

42. (1) Any court of competent jurisdiction shall try any offence under this Act where the act or omission constituting the offence is committed in Kenya.

(2) For the purposes of subsection (1), an act or omission committed outside Kenya which would if committed in Kenya constitute an offence under this Act is deemed to have been committed in Kenya if—

(a) the person committing the act or omission is—

(i) a citizen of Kenya; or

(ii) ordinarily resident in Kenya; and

(b) the act or omission is committed—

(i) against a citizen of Kenya;

(ii) against property belonging to the Government of Kenya outside Kenya; or

(iii) to compel the Government of Kenya to do or refrain from doing any act; or

(c) the person who commits the act or omission is, after its commission or omission, present in Kenya.

Forfeiture.

43. The court before which a person is convicted of any offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, device or thing to the Authority which is the subject matter of the offence or is used in connection with the commission of the offence.

Prevailing Clause.

44. Whenever there is a conflict between this Act and any other law regarding cybercrimes, the provisions of this Act shall supersede any such other law.

Consequential Amendments. Cap 411A

45. The law specified in the first column of the Schedule is amended, in the provisions specified in the second column thereof, in the manner respectively specified in the third column.

46. The Cabinet Secretary may make Regulations for the better carrying out of the provisions of this Act. Regulations.

SCHEDULE (s.45)

Written law	*Provision*	*Amendment*
Kenya Information and Communication Act, 1998	83U	Repeal
	83V	Repeal
	83W	Repeal
	83X	Repeal
	83Z	Repeal
	84A	Repeal
	84B	Repeal
	84F	Repeal

MEMORANDUM OF OBJECTS AND REASONS

Statement of Objects and Reasons of the Bill

The Bill proposes to provide a framework to prevent and control the threat of cybercrime, that is, offences against computer systems and offences committed by means of computer systems.

Kenya Vision 2030 recognizes ICT as one of the key drivers of socio-economic development in the Republic and an enabler in achieving the middle income country status. The Bill is intended to protect and ensure a secure and safe digital environment.

The structure of the Bill is as follows—

PART I (Clause 1-3) Provides for preliminary matters including the short title and interpretation of terms as used in the Bill. This Part also provides for the objects of the Bill.

PART II (Clause 4-21) Outlines cyber related offences and penalties. Offences outlined include; unauthorised access, access with intent to commit or facilitate further offence, unauthorised interference, unauthorised interception, illegal devices codes, unauthorised disclosure of password or access code, enhanced penalties for offences involving protected computer system, cyber espionage, false publications, child pornography, computer forgery, computer fraud, cyber stalking and cyber bullying, aiding or abetting in the commission of an offence, offences by a corporate and limitation of liability, recovery of assets, and offences committed through the use of a computer system. This part also gives guidelines on compensation order by courts upon conviction for offences outlined under this part.

PART III (Clause 22-32) Provides for investigation procedures including search and seizure of stored computer data, such power to search without warrant in special circumstances, record of and access to seized data, production order and grounds for such application of a production order by a police officer, expedited preservation and partial disclosure of traffic data, such period for preservation and extension of the said period. More procedures detailed are real time collection of traffic data, interception of content data, procedure for making application to intercept and such grounds to be satisfied before such interception. This Part also provides for confidentiality of investigations and powers to deal with obstruction of investigations.

PART IV (Clause 33-41) This Part provides for International cooperation and contains provisions relating to trans-boarderborder and international cooperation.

PART V (Clause 42-46) Contains the general provisions including territorial jurisdiction, forfeiture, consequential amendments and the power to make regulations.

Statement on the delegation of legislative powers and limitation of fundamental rights and freedoms.

This Bill delegates regulation-making powers to the Cabinet Secretary responsible for matters relating to Information, Communication and Technology. The Bill does not contain provisions limiting rights and fundamental freedoms.

Statement that the Bill does not concern county governments

This Bill is not a Bill concerning counties within the meaning of Article 110 of the Constitution.

Statement that the Bill is not a money Bill within the meaning of Article 114 of the Constitution

The enactment of this Bill shall not occasion additional expenditure of public funds.

Dated the 7th June, 2017.

ADEN DUALE,
Leader of the Majority Party.