THE CYBERCRIME AND COMPUTER RELATED CRIMES BILL, 2014

AS PROPOSED BY

THE OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS (ODPP)

THE CYBERCRIME AND COMPUTER RELATED CRIMES BILL, 2014

ARRANGEMENT OF CLAUSES

Clauses

PART-IV-CONTENT RELATED OFFENCES

PART V – PROCEDURES AND INVESTIGATIONS

PART VI –GENERAL PROVISIONS

AN ACT of Parliament to prohibit unauthorized access, use or interference with a computer; to protect the integrity of computer systems and the confidentiality, integrity and availability of data; to prevent abuse of computer systems; to facilitate the gathering and use of electronic evidence; and connected purposes

ENACTED by the Parliament of Kenya—

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the Cybercrime and Computer related Crimes Bill, 2014.

Interpretation.

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

"access" in relation to any computer system", means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system;

"computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device or collection of devices including input and output devices but excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions and data that perform logic, arithmetic, data storage, data retrieval, communication control and other functions;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(a) causes any loss;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care

of one or more persons;
(c) causes or threatens physical injury or death to any person; or
(d) threatens public health or public safety;

"data" means information recorded in a format in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

"electronic device", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"electronic form" with reference to information, means any information generated, sent, received or stored in magnetic, optical, computer memory, microfilm or similar device;

"electronic record" means a record generated in digital form by an information system, which can be transmitted within an information system or from one information system to another and stored in an information system or other medium;

"equipment" includes any appliance, apparatus or accessory used or intended to be used for communication services;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"intercept in relation to a function of a computer", includes listening to, or recording a function of a computer, or acquiring the substance, its meaning or purport of such function;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information and communication technologies" means technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any

telecommunication system;

"modification" means a modification of the contents of any computer system by the operation of any function of that computer system or any other computer system as a result of which—

(*a*) any program or data held in the computer system is altered or erased;

(*b*) any program or data is added to its contents; or

(*c*) any act occurs which impairs the normal operation of the computer system;

"offence" in this Act, means an offence against a provision of any law in Kenya, or an offence against a provision of any law in a foreign state for conduct which, if it occurred in Kenya, would constitute an offence against a provision of any law in Kenya;

"person" includes any company or association or body of persons corporate or unincorporate;

"program" or **"computer program**" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"traffic data" means any computer data relating to 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 type of underlying service.

PART II—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

Unauthorized access to computer data

3. (1) Subject to subsections (2) and (3), a person who causes a computer system to perform a function, knowing that the access they intend to secure is unauthorised, commits an offence and shall on conviction be liable to a fine not exceeding five hundred thousand shillings or to three years imprisonment or both

(2) Access by a person to any program or data held in a computer is authorised if—

(a) that person has the right to control the operation or use of the computer system and exercises such right in good faith;

(b) that person has the express or implied consent of the person, empowered to authorise them, to have such an access;

(c) that person has reasonable grounds to believe that they had such consent as specified in paragraph (b);

(d) that person is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

(3) An access by a person to a computer system is unauthorised if–

(a) that person is not himself entitled to control access of the kind in question; and

(b) does not have consent to access by him of the kind in question from any person who is so entitled.

(4) 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 offences.

4. (1) A person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system, with intent to commit an offence under any law, that person commits an offence and is liable upon conviction to a fine not exceeding five hundred thousand shillings or to imprisonment term of two years or both.
(2) For the purposes of this section, it is immaterial that—

(*a*) the access referred to in subsection (1) is authorized or unauthorized;

(*b*) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorized modification of computer data.

5. (1) A person who intentionally and without right—

(a) does any act which causes an unauthorised modification of

the computer data; and

(2)Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, the person convicted of such offence is liable on conviction to a fine not exceeding two hundred thousand shillings or to imprisonment for a term of two years or both.

(3) For purposes of this section modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from a person who is entitled.

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

Unauthorized access to and interception of computer service.

6. (1) Subject to subsection (2), a person who by any means knowingly:—

(*a*) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service;

(*b*) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, commits an offence is liable upon conviction to a fine not exceeding five hundred thousand shillings or to an imprisonment term of three years or both.

(2)Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, the person convicted of such offence is liable on conviction to a fine not exceeding two hundred thousand shillings or to imprisonment for a term of two years or both.

(3) For the purpose of this section, it is immaterial that the unauthorized access or interception 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.

(4) A person is not be liable under subsection (1) if—

(*a*) that person has the express or implied consent of both the person who sent the data and the intended recipient of such data;

(*b*) is acting in reliance of any statutory power.

Damaging or denying access to computer system.

7. (1) A person who without lawful authority or lawful excuse, does an act which causes directly or indirectly –

(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or

(b) a denial of access to, or impairment of any program or data stored in, the computer system, commits an offence and shall be liable upon conviction to a fine not exceeding five million shillings or to an imprisonment term of three years or to both.

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

Unauthorized disclosure of access code.

8. (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and fifty thousand shillings or to an imprisonment term of three years or to both.

System interference.

9. A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred and fifty thousand shillings or to an

imprisonment term of three years or to both.

Illegal devices or data.

10. A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a computer system or any other device or an designed or adapted primarily for the purpose of committing any offence under sections 1 to 9, shall commit an offence.

(2) A person who knowingly receives, or is in possession, without sufficient excuse or justification, of one or more of the devices under subsection (1) commits an offence.

(3) A person who is found in possession of any data or program with the intention that the data or program be used, by the person himself or another person, to commit or facilitate the commission of an offence under this Act, also commits an offence.

(4) For the purposes of subsection (3), possession of any data or program includes—

(*a*) having possession of a computer system or data storage device that holds or contains the data or program;

(*b*) having possession of a document in which the data or program is recorded; or

(*c*) having control of data or program that is in the possession of another person.

(5) A person who commits an offence under this section is liable upon conviction to a fine not exceeding one million shillings or to an imprisonment term of three years or to both.

Unauthorized receiving or giving access to a computer program or data.

11. (1) A person who receives or is given access to any program or data held in a computer and who is not authorised to receive or have access to that program or data whether or not the person knows that the person giving him the program or data has obtained that program or data through authorised or unauthorised means, commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to imprisonment term of two years, or to both.

(2) A person who is authorised to receive or have access to any

program or data held in a computer and who receives that program or data from another person knowing that the other person has obtained that program or data through unauthorised means commits an offence and is liable on conviction to a fine not exceeding one million shillings or to imprisonment term of three years, or to both.

(3) A person who has obtained any program or data held in a computer through authorised means and gives that program or data to another person who the person knows is not authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to an imprisonment term not exceeding three years, or to both.

(4) A person who has obtained any program or data held in a computer through unauthorised means and gives that program or data to another person whether or not the person mows that that other person is authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding five hundred thousand shillings or to imprisonment for a term not exceeding two years, or to both.

PART III—COMPUTER RELATED OFFENCES

Computer related forgery.

12. (1) A person who intentionally and without lawful excuse or justification, inputs, alters, delays transmission, 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, commits an offence and is liable upon conviction to a fine not exceeding ten million or ten years imprisonment or both.

(2) For purposes of subsection (1), it is immaterial whether or not the data is directly readable and intelligible.

Computer related fraud.

13. A person who intentionally and without lawful excuse or justification, causes the loss of property to another by—

(a) any input, alteration, deletion, delaying transmission or suppression of computer data;

(b) any interference with the functioning of a computer system,with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, commits an

offence and is liable upon conviction to a fine not exceeding five million or ten years or both.

Unauthorized access to protected system

14. A person who secures access or attempts to secure access to a protected system or computer in contravention of the provisions of this Part commits an offence and is liable upon conviction to a fine not exceeding one million shillings or an imprisonment term of five years, or both.

PART IV—CONTENT RELATED OFFENCES

Child pornography.

Cap no. 3 of

15. (1) Subject to section 16 (2) of the Sexual Offences Act, 2006, a person who—

(a) sells, lets to hire, distributes, publicly exhibits through a computer system and puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or their possession any obscene book, pamphlet, paper, drawing, painting, art, representation or figure or any other obscene object;

(b) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited through a computer system and put into circulation;

(c) takes part in or receives profits from any business in the course of which they know or has reason to believe that any such obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited through a computer system and put into circulation;

(d) advertises or makes known through a computer system that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person;

(e) offers or attempts to do any act which is an offence under this section, commits an offence of child pornography and is liable upon conviction is liable to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, for imprisonment to a term of not less than seven years without the option of a fine.

(2)For the purposes of subsection (1), a book, pamphlet, paper,

drawing, painting, art, representation or figure or any other object shall be considered to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or where it comprises two or more distinct items the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(3) For purposes of this section, child pornography also includes pornographic material that visually depicts—

(a) a minor engaging in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct. ☐

Hate speech.

16. (1) A person who—

(a) uses threatening, abusive or insulting words or behaviour,

(b) displays any written or electronic material;

(c) publishes or distributes written or electronic material; or

(d) distributes, shows or plays, a recording of visual images;

through a computer system which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behaviour whether publicly or anonymously, commits an offence if that person intends to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up.

(2)It is immaterial where the offence referred to in subsection (1) is conducted privately or publicly.

(3) A person who commits an offence under this section shall be liable upon conviction to a fine not exceeding one million shillings or to an imprisonment term for a term not exceeding five years or to both. In this section, "ethnic hatred" means hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

Identity related crimes.

17. (1) A person who, intentionally and without lawful excuse or justification by using a computer system at any stage of the offence, transfers, possesses, or uses any means of identification of another person, with the intent to commit, aid

or abet, in connection with, any unlawful activity that constitutes a crime, commits an offence.

(2) A person is liable upon conviction under subsection (1) to a fine not exceeding five hundred thousand shillings or to an imprisonment term of five years or both.

Cyberstalking

18. (1) A person who willfully, maliciously, and repeatedly uses a computer system including electronic communication to harass, intimidate or cause substantial emotional distress or anxiety to another person—

(a) makes a threat with the intent to place that person in reasonable fear for their safety or to a member of that person's immediate family;

(b) communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image;

(c) make any suggestion or proposal of an obscene nature;

(d) threaten any illegal or immoral act;

(e) take or distribute pictures or photographs of any person without his consent or knowledge;

(f) display or distribute information in a manner that substantially increases the risk of harm or violence to any other person,

commits the offence of cyber stalking.

(2) A person who is convicted of the offence referred to in section (1) is liable to a fine not exceeding three hundred thousand shillings or to an imprisonment term of three years or both.

(3) If the offence referred to in subsection (1) involves a minor, the penalty is a fine not exceeding five hundred thousand shilling s or to an imprisonment term of ten years or both.

Phishing.

19. (1) A person who establishes a website, or sends an electronic message with a counterfeit source intended to deceive the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later may be used for unlawful purposes commits the offence of` phishing.

(2) A person who commits an offence of phishing upon conviction is liable to a fine not exceeding five hundred

thousand shillings or to an imprisonment term of three years or both.

(3) Where the phishing attack results in economic gain for the sender, the penalty upon conviction is a fine not exceeding five million shillings or an imprisonment term of seven years or both.

Spamming

20. (1) A person who, intentionally without lawful excuse or justification—

(a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system;

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,

commits an offence is liable upon conviction to an imprisonment term for a period not exceeding three years, or to a fine not exceeding five hundred thousand shillings or to both.

(2) This section shall not apply to the transmission of multiple electronic messages within customer or business relationships.

Offences by body corporate.

21. (1) Where a body corporate is held liable for an offence under this Act if the offence is committed on its instructions or for its benefits. The body corporate shall be punished with fine not exceeding fifty million shillings or the amount involved in the offence whichever is the higher.

(2) Where a corporation is convicted of an offence, or is fined under this Act, any person who is a director of, or who is concerned in the management of that corporation shall be considered to have committed the same offence and is liable to be fined as if the person authorized or permitted the same or omission constituting the offence—

(3) Where at the trial of a corporation for an offence under this Act, a director or any person concerned in the management of that body corporate shows that—

(a) the act constituting the offence was done without the knowledge or consent of that director or person; or

(b) the director or person took, reasonable steps to prevent the act from being committed;

the director or person shall not be liable.

Abatements and attempts.

22. (1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

(2) A person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

Attempts.

23. (1) When a person, intending to commit an offence, begins to put their intention into execution by means adapted to its fulfilment, and manifests their intention by some overt act, but do not fulfil their intention to such an extent as to commit the offence, they are considered to attempt to commit the offence.

(2) It is immaterial, whether the person does all that is necessary on their part for—

(a) completing the commission of the offence;

(b) whether the complete fulfillment of their intention is prevented by circumstances independent of their will; or

(c) whether they desists of their own motion from the further prosecution of

their intention.

(3) It is immaterial that by reason of circumstances not known to the offender it is impossible in fact to commit the offence

PART V—PROCEDURES AND INVESTIGATIONS

Powers of access, search and seizure

24. (1) Where a court is satisfied on the basis of an application by a Police officer or lawful authority supported by information on oath that there are reasonable grounds to believe that there may be in a place a thing or computer data—

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence.

(2)On the basis of an application made under subsection (1), the court may issue a warrant authorizing a police Officer or lawful authority, to enter any premises to access, search and seize the thing or computer data including—

(i) a computer system or part of it and computer data stored therein; and

(ii) a computer-data storage medium in which computer data may be stored in the territory of the country.

(3) Where a police officer or lawful authority acting under a warrant issued under subsection (2) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the police officer or lawful authority must expeditiously extend the search or access to the other system.

(4) A Police Officer or lawful authority undertaking a search under this section is empowered to seize or secure data accessed.

Preservation order.

25. (1) A police officer or lawful authority may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court considers appropriate.

Expedited preservation.

26. (1) If a police officer or lawful authority is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the police officer may, by written notice given to a person in control of the data, require the person to ensure that the data specified in the notice be preserved for a period of up to ninety (90) days as

specified in the notice.

(2) The period may be extended beyond ninety days upon an application a court authorizes an extension for a further specified period of time.

(3) A preservation notice comes into force when the carrier receives the directive or order as the case may be.

Disclosure of data.

27. A police officer or lawful authority may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved or specified data stored or processed by means of a computer system or any other information and communication technologies, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted.

Production order.

28. (1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer or lawful authority may apply to court for an order compelling—

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

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

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be considered to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Collection of traffic data.

29. (1)If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds to suspect or believe

that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the court may order a person in control of such data to—

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified law enforcement officers to collect or record that data.

(2)If a court is satisfied on the basis of an application by a police officer or lawful, supported by information on oath that there are reasonable grounds to suspect or believe that traffic data is reasonably required for the purposes of a criminal investigation, the court may authorize the police or prosecutions officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of traffic data.

30. If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds that traffic data is reasonably required for the purposes of a criminal investigation, the court may authorize a police officer or lawful authority to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Obligation to report data loss.

31. (1) All public or private corporations processing personal data shall as soon as practicable report any security breaches resulting in theft, loss or misuse of data to the police.

(2) A public or private corporation who fails to comply with subsection (1) commits an offence.

Interception of content data.

32. If a court is satisfied on the basis of an application by a police officer or lawful authority supported by information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the court may—

(a) order a service provider whose service is available in Kenya through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a police officer or lawful authority to collect or record that data through application of technical means.

Forensic tools.

33. (1) If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath that in a criminal investigation concerning an offence under this Act, there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments and is reasonably required for the purposes of a criminal investigation, the court may authorize the police officer or lawful authority to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information—

(a) suspect of the offence, if possible with name and address;

(b) description of the targeted computer system;

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

(2) Within such investigation, the police officer or lawful authority must ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation process it is necessary to—

(a) the technical mean used and time and date of the application;

(b) the identification of the computer system and details of the modifications undertaken within the investigation;

(c) any information obtained.

(3) Information obtained by the use of such tool need to be protected against any modification, unauthorized deletion and unauthorized access.

(4) The duration of authorization in this subsection (1) is limited to nine months. If the conditions of the authorization are no longer met, the actions taken are to stop immediately.

(5) The authorization to install the tool includes remotely accessing the suspect's computer system.

(6) If the installation process requires physical access to a place the requirements of section 23 need to be fulfilled.

(7) If necessary a police officer may pursuant to the order of court granted in subsection (1) request a service provider to support the installation process.

Duty to cooperate.

34. (1) A person who is required to cooperate with police or lawful authority in their discharge of functions under this Act or any other written law, and shall in particular—

(a) respond to any inquiry;

(b) comply with any lawful directions including disclosing access code to a computer system or computer; and

(c) furnish such information as may be required;

(2) A person who contravenes subsection (1) is be liable upon conviction, to an imprisonment term of one year or to a fine not exceeding three hundred thousand shillings or to both.

(3) In addition to the penalty prescribed under subsection (2), a public officer or State officer may be subjected to the relevant disciplinary procedures.

PART VI—GENERAL PROVISIONS

Jurisdiction

35. The Kenyan courts shall have jurisdiction where an act done or an omission made constituting an offence under this Act has been committed—

(a) in the territory of Kenya;

(b) by a national of Kenya outside the territory of Kenya

(c) on a ship or aircraft registered in Kenya;

(d) in part in Kenya;

(e) using a Kenyan domain name; or

(f) outside the territory of Kenya and where any result of the offence has an effect in Kenya.

Admissibility of electronic evidence.

36. The fact that evidence has been generated from a computer system does not by itself prevent that evidence from being admissible.

Confiscation of assets.

37. A court may order the confiscation of moneys, proceeds, properties and assets purchased or obtained by a person with proceeds derived from or in the commission of an offence under this Act and may further make an order of restitution.

International cooperation.

38. The Provisions of the Mutual Legal Assistance Act, 2011shall apply to this Act.

Protection from personal liability.

39. No act done by a person exercising a function in this Act shall, if the act was done in good faith for the purpose of carrying out the provision of this Act, subject the person to any liability, action, claim or demand.

General penalty.

40. A person who contravenes any provisions of this Act commits an offence and shall be liable upon conviction to a fine of not exceeding two million shillings or to imprisonment term of three years or both.

Regulations.

41. The Cabinet Secretary for the time being responsible for matters relating to information, communication and technology may, in consultation with the Director of Public Prosecutions make regulations regarding any matter provided under this Act.