BELIZE:

CYBERCRIME BILL, 2020

ARRANGEMENT OF CLAUSES

PART I

Preliminary

PART II

Cybercrime Offences

PART IV

International Cooperation

PART V

Miscellaneous

BELIZE:

BILL

for

AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto.

(Gazetted ....., 2020)

BE IT ENACTED, by and with the advice and consent of the House of Representatives and the Senate of Belize and by the authority of the same, as follows:

PART I

Preliminary

Short title.

1. This Act may be cited as the

CYBERCRIME ACT, 2020.

Interpretation.

2.–(1) In this Act–

Act No. 8 of 2014.

"Central Authority" means the Central Authority designated under the Mutual Legal Assistance Act;

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

Act No. 3 of 2013.

"child pornography" has the meaning assigned to it under the Commercial Sexual Exploitation of Children Act;

"Court" means the Supreme Court acting in its criminal jurisdiction;

"communication" means–

(a) anything encrypted or unencrypted comprising of speech, music, sounds, visual images or data of any description; and

(b) encrypted or unencrypted signals serving for the impartation of anything–

(i) between persons, a person and a thing or between things; or

(ii) for the actuation or control of any apparatus;

"communication data" means any-

(a) encrypted or unencrypted data comprised in or attached to a communication whether by the sender or otherwise, for the purpose of a communication network by means of which the communication is transmitted;

(b) encrypted or unencrypted information, that does not include the contents of a communication, other than data that falls within paragraph (a), that is made by a person–

(i) of any communication network; or

(ii) any part of a communication network in connection with the provision to or use by any person of any communication service;

(c) encrypted or unencrypted information that does not fall within paragraph (a) or (b) that is held or obtained by a person providing a communication service in relation to a person to whom the service is provided;

"communication network" means any wire, radio, optical or other electromagnetic system used to route switch or transmit communication;

"communication service" means a service that consists in the provision of access to and of facilities for making use of, any communication network, whether or not it is one provided by the person providing the service;

"computer data" means any representation of–

(a) facts;

(b) concepts;

(c) machine-readable code or instructions; or

(d) information, including text, audio, image or video,

that is in a form suitable for processing in a computer system and is capable of being sent, received or stored;

"computer programme" means computer data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

"computer system" means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of computer data, including a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, a smart phone, a personal digital assistant, or a smart television;

"damage" means any impairment to the integrity or availability of data, a program, a computer system, communication network or information;

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

"Minister" means the Minister with responsibility for national security;

"person" includes a natural or legal person, an educational or financial institution or any legal or other entity;

"security measure" means password, access code, encryption code or biometric information in the form of computer data and includes any means of limiting access to authorised persons or to secure recognition prior to granting access to communication data, a communication network, a computer system or computer data;

"service provider" means–

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or

(b) any public or private entity that processes or stores computer data on behalf of a communication service or users of the service;

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

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

(b) the subscriber's identity, postal or geographic 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 communication equipment available on the basis of the service agreement or arrangement;

"Storage Direction" means any Order of a court compelling a service provider to store and make available to a stipulated party a person's stored traffic data and subscriber information; and

"traffic data" means any communication data–

(a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication that is, may be or may have been transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article;

(b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted;

(c) comprising signals for the actuation of–

(i) apparatus used for the purpose of a communication network for effecting, in whole or in part, the transmission of any communication; or

(ii) any communication network in which that apparatus is comprised;

(d) identifying the data or other data as data comprised in or attached to a particular communication; or

(e) identifying a computer file or a computer programme, access to which is obtained or which is run by means of the communication,

to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and a reference to traffic data being attached to a communication includes a reference to the data and the communication being logically associated with each other.

PART II

Cybercrime Offences

Illegal access to a computer system.

3.–(1) A person commits an offence who, intentionally accesses a computer system or any part of a computer system of another person –

(a) without authorisation or in excess of authorisation; or

(b) by infringing any security measure of the computer system.

(2) A person commits an offence who intentionally and without lawful excuse or justification continues to exceed the authorised access to the computer system of another person.

(3) A person who commits an offence under this section is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years;

(b) conviction on indictment to a fine of five thousand dollars and to a term of imprisonment for five years.

Illegal access to computer data.

4.–(1) A person commits an offence who, without authorisation accesses the computer system of another person with the intention to duplicate or modify the data–

(a) without authorisation or in excess of authorisation; or

(b) by infringing a security measure.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Illegal data interference.

5.–(1) A person commits an offence who, intentionally and without lawful excuse or justification–

(a) damages the computer data of another person;

(b) obstructs, interrupts or interferes with another person's lawful use of computer data; or

(c) denies access to computer data to another person who is authorised to access the computer data.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Illegal system interference.

6. –(1) A person commits an offence who, intentionally and without lawful excuse or justification, seriously hinders or interferes with the functioning of the computer system of another person by inputting, transmitting, damaging, modifying or suppressing computer data.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years, or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

(3) For the purposes of this section "seriously hinders" includes–

(a) disconnecting the electricity supply to the computer system;

(b) causing electromagnetic interference to the computer system; or

(c) corrupting the computer system.

Illegal devices and codes.

7.–(1) A person commits an offence who, for the purpose of committing an offence under this Act or any other law, intentionally and without lawful excuse or justification, possesses, procures for use, produces, sells, imports or exports, distributes, discloses or otherwise makes available–

(a) a device or a computer programme, that is designed or adapted; or

(b) a security measure by which the whole or any part of a computer system or computer data is capable of being accessed.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Computer related forgery.

8. A person commits an offence who, intentionally inputs, modifies or suppresses computer data, regardless of whether or not the data is directly readable and intelligible, and the input, modification or suppression causes the data to become inauthentic–

(a) is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) on conviction on indictment to a fine of five thousand dollars and to a term of imprisonment for five years.

Identity related fraud.

9.–(1) A person commits an offence who, with the intent to defraud or deceive another person for the purpose of procuring an economic benefit for the person or another–

(a) inputs, alters, deletes or suppresses computer data; or

(b) interferes with the functioning of a computer system.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or

(b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years.

Identity related fraud, theft.

10.–(1) A person commits an offence who, with the intent to assume the identity of another person, uses a computer system or computer data to–

(a) obtain, transfer, possess or use a means of identification of another person; or

(b) make use of the security measures of another person.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Child luring.

11.–(1) A person commits an offence who, uses a computer system to communicate with a child with the intent to –

(a) induce the child to engage in a sexual conversation or sexual activity with the child; or

(b) encourage the child to produce child pornography; or

(c) arrange a meeting with a child for the purpose of abusing or engaging in sexual activity with the child, or producing child pornography, whether or not the person takes any steps to effect the meeting.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years, or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Publication or transmission of image of private area.

12.–(1) A person commits an offence who, without the explicit consent of another person, intentionally captures, stores in, publishes or transmits through a computer system, an image of a private area of the other person and is liable–

(a) on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) on conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

(2) For the purposes of this section, "private area" means genitalia, buttocks or breasts.

(3) Notwithstanding the penalty under sub-section (1), a Court may, by Order prohibit the offender from using the internet or any computer system and impose any conditions on the offender as determined by the Court.

(4) An Order under sub-section (3) shall be for any period the Court considers appropriate, including any period of imprisonment imposed on the offender.

(5) A prosecutor or an offender may apply to the Court for a variation of any condition under the Order.

(6) Where the Court determines that there is a change in the circumstances of the case, the Court may vary the conditions of the Order.

No liability for service provider.

13.–(1) A service provider or a user of the service provider's service, shall not be deemed a publisher or speaker of any information that is provided by another service provider or user.

(2) A service provider or user shall not be liable for–

(a) any action taken to enable or make available to a subscriber or user, the technical means to restrict access to any material described under paragraph *(b)*; or

(b) any action voluntarily taken in good faith to restrict access to or availability of material which the service provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not the material is constitutionally protected.

Service provider to store traffic data and subscriber information.

14.–(1) A service provider shall store and keep the traffic data of subscribers from the date on which the data is generated by a computer system until ninety days after the determination of a service agreement with a customer.

(2) A service provider who fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for one year.

Using a computer system to coerce, harass, intimidate, etc. a person.

15. –(1) A person commits an offence who, with intent to compel another person to do or refrain from doing any act, uses a computer system to publish or transmit computer data that–

(a) intimidates the other person;

(b) threatens the other person with violence or damage to property; or

(c) threatens a member of the other person's family with violence.

(2) For the purposes of this section "intimidate" means –

(a) to cause in the mind of a reasonable person an apprehension of injury to the person, to a member of the person's family or a to dependant of the person, or of violence or damage to the person's property; or

(b) to cause a person substantial emotional distress.

(3) A person commits an offence who, uses a computer system to–

(a) publish or transmit computer data that is obscene, vulgar, profane, lewd, lascivious or indecent, with intent to–

(i) humiliate, harass or cause substantial emotional distress to another person; or

(ii) cause the other person to be subject to public ridicule, contempt, hatred or embarrassment

(b) repeatedly send to another person, computer data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate or harass the other person, and the humiliation or harassment is detrimental to the health, emotional well-being, self-esteem or reputation of the other person.

(4) A person commits an offence who, uses a computer system to disseminate any information, statement or image, knowing the information, statement or image to be false, with the intent to cause–

(a) harm to the reputation of the other person; or

(b) the other person to be subject to public ridicule, contempt, hatred or embarrassment.

(5) A person commits an offence who, uses a computer system to threaten to publish computer data containing personal or private information of another person, with the intent to–

(a) extort a benefit from the other person; or

(b) cause the other person public ridicule, contempt, hatred or embarrassment.

(6) A person who commits an offence under this section is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for five years.

Infringement of copyright, patents and designs and trademarks.

16.–(1) A person commits an offence who, uses a computer system to infringe on the rights of–

(a) a copyright owner;

(b) a proprietor of a patent;

(c) a proprietor of a registered design; or

(d) a proprietor of a registered trademark.

(2) A person who commits an offence under sub-section (1), is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years.

Attempt, aiding or abetting**.**

17.–(1) A person commits an offence who, intentionally–

(a) advises, incites, attempts, aids, abets, counsels, procures or facilitates the commission of any offence under this Act; or

(b) conspires with another person to commit an offence under this Act.

(2) A person who commits an offence under sub-section (1), is liable for the offence as if the person is the principal offender.

Offences prejudicing investigation.

18.–(1) A person commits an offence who, knows or has reasonable grounds to believe that an investigation in relation to an offence under this Act is being or is about to be conducted, and who intentionally–

(a) makes a disclosure that is likely to prejudice the investigation; or

(b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents or computer data that are relevant to the investigation.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

(3) Notwithstanding sub-section (1), it is a defence under sub-section (1)(a) if–

(a) the accused does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;

(b) the disclosure is made in the exercise of a function under this Act or in compliance with a requirement imposed under or by virtue of this Act;

(c) the accused is an attorney-at-law and the disclosure is–

(i) to a client in connection with the giving of legal advice to the client; or

(ii) to any person in connection with legal proceedings or contemplated legal proceedings.

(4) Notwithstanding sub-section (1), it is a defence under sub-section (1)*(b)* if the accused –

(a) does not know or suspect that the documents or computer data are relevant to the investigation; or

(b) does not intend to falsify, conceal, destroy or otherwise dispose of any facts disclosed by the documents or computer data, from any official carrying out the investigation.

(5) Notwithstanding sub-section (2)*(c)(ii)*, a person commits an offence if the disclosure is made in furtherance of a criminal purpose.

PART III

Enforcement

Ex-parte application for Storage Direction.

19.–(1) The Director of Public Prosecutions or Head of Prosecution Branch may in the prescribed form, make an *ex-parte* application for a Storage Direction.

(2) An application under sub-section (1), shall–

(a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(i) the name of the investigating police officer;

(ii) the facts or allegations giving rise to the application, including the alleged offence;

(iii) sufficient information for the Court to make a determination on whether to grant or refuse the application;

(iv) the ground on which the application is made;

(v) full particulars of all facts and circumstances alleged, including–

(aa) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the traffic data and subscriber information are to be intercepted; and

(bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the life/period of the Storage Direction,

(vi) where applicable–

(aa) whether other investigative procedures were applied and whether they failed to produce the required evidence; or

(bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(vii) the requested duration of the Storage Direction;

(viii) whether any previous application was made for a Storage Direction in respect of the person, facility or premises, and the status of that other application;

(ix) where applicable, a description of the computer system to be targeted; and

(x) any other relevant directives issued by a Court in relation to the matter.

(3) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs, an application for a Storage Direction, shall not require the grounds under section 22(1)*(a).*

(4) Where a Storage Direction is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.

(5) Records relating to an application for a Storage Direction, renewal or modification of a Storage Direction, shall immediately upon the determination of the matter, be–

(a) sealed by the Court; and

(b) kept in the custody of the Court, in a place that is not accessible to the public, or in any other place as the Court determines fit.

(6) The records under sub-section (5) may be unsealed upon an order by the Court for the following purpose only–

(a) on an application for a further Storage Direction, in relation to the same matter; or

(b) for a renewal of a Storage Direction.

Scope and form of Storage Direction.

20.–(1) A Storage Direction shall direct the named service provider to–

(a) keep stored, at any place in Belize accurate records of–

(i) the traffic data and subscriber information of any person, facility or premises;

(ii) any computer system; or

(iii) any communication in the course of its transmission;

(b) store the traffic data for the period of time as stated in the Storage Direction; and

(c) submit the stored traffic data and subscriber information to a named police officer.

(2) A Storage Direction shall specify–

(a) the manner in which the data is to be stored and submitted to the police officer; and

(b) any other conditions or restrictions that relate to the traffic data.

(3) A Storage Direction may contain any ancillary provisions as may be necessary to secure its implementation in accordance with the provisions of this Act.

Ex-parte application for Search and Seizure Warrant.

21.–(1) The Director of Public Prosecutions or Head Prosecution Branch may in the prescribed form, make an *ex-parte* application for Search and Seizure Warrant.

(2) An application under sub-section (1), shall–

(a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(i) the name of the investigating police officer;

(ii) that there is reasonable grounds for suspecting that–

(aa) an offence under this Act or any other law has been or is about to be committed, in a specified place; and

(bb) evidence that the offence has been or is about to be committed, is in the specified place.

(iii) the facts or allegations giving rise to the application, including the alleged offence;

(iv) sufficient information for the Court to make a determination on whether to grant or refuse the application;

(v) the ground on which the application is made;

(vi) full particulars of all facts and circumstances alleged, including–

(aa) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the traffic data and subscriber information are to be intercepted; and

(bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the duration of the Search and Seizure Warrant;

(vii) where applicable–

(aa) whether other investigative procedures were applied and whether they failed to produce the required evidence; or

(bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(viii) The requested duration of the Search and Seizure Warrant;

(ix) whether any previous application was made for a Search and Seizure Warrant in respect of the person, facility or premises, and the status of that other application;

(x) where applicable, a description of the computer system to be targeted; and

(xi) any other relevant directives issued by a Court in relation to the matter.

(3) A Search and Seizure Warrant shall specify the place, or evidence to which it relates and authorise a police officer, with any assistance as the police officer deems necessary, to–

(a) enter and search any place; or

(b) to access, seize and secure any evidence, including any computer system or computer data.

(4) A police officer who executes a Search and Seizure Warrant under this section shall, secure the computer system or data and maintain the integrity of the data seized.

(5) In addition to any powers of a Search and Seizure Warrant under this section, a police officer when executing a Search and Seizure Warrant, has the following additional powers including–

(a) to activate an onsite computer system;

(b) inspect and check the operation of a computer system or computer data;

(c) to make and retain a copy of computer data;

(d) to remove computer data from a computer system or render the computer system inaccessible;

(e) to take a printout of computer data; or

(f) to impound or similarly secure a computer system or any part of the system.

(6) Any evidence seized under a Search and Seizure Warrant, including any computer system or data shall be valid for a period of ninety days and may, on an application to a Judge in Chambers, be extended for a further period of not more than one year.

(7) Upon the expiration of the period stated under sub-section (6), or when the evidence seized is no longer required, the evidence shall immediately be returned to the person to whom the Search and Seizure Warrant was addressed.

(8) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs, an application for a Storage Direction, shall not require the grounds under section 22(1)*(a).*

(9) Where a Search and Seizure Warrant is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.

Application for a Storage Direction or Search and Seizure Warrant**.**

22.–(1) A Court shall issue a Storage Direction or a Search and Seizure Warrant, where it is satisfied that the facts deponed there is reasonable grounds to believe that–

(a) obtaining the information sought is necessary in the interest of–

(i) national security;

(ii) public order;

(iii) public safety;

(iv) public health;

(v) preventing, detecting, investigating or prosecuting an offence under this Act or any other law; or

(vi) giving effect to the provisions of any mutual legal assistance request or in circumstances appearing to the Court to be equivalent to those in which he would issue a Storage Direction under sub-paragraph *(v)*; and

(b) other procedures–

(i) have not been or are unlikely to be successful in obtaining the information sought;

(ii) are too dangerous to adopt in the circumstances; or

(iii) are impractical having regard to the urgency of the case; or

(c) it would be in the best interest of the administration of justice to issue the Storage Direction.

(2) In considering an application under sub-section (1), the Court may require the applicant to furnish the Court with any further information as it deems necessary.

Extension of time for prosecution of an offence.

23. Notwithstanding the provisions of any written law prescribing the time within which proceedings for an offence punishable on summary conviction may be commenced, summary proceedings for an offence under this Act, or for attempting to commit, conspiring with another person to commit, or soliciting, inciting, aiding, abetting or counselling or causing or procuring the commission of, such an offence, or for attempting to solicit, incite, aid, abet, counsel or cause or procure the commission of such an offence, may be commenced within twelve months of the commission of the offence,

provided that where the offence is punishable on summary conviction and on conviction on indictment, nothing in this section shall be deemed to restrict the power to commence, after the expiry of the aforesaid period of twelve months, proceedings for conviction on indictment for that offence or for any other act, relating to the offence, referred to in this section.

Record of material seized.

24.–(1) A police officer who seizes or renders a computer system inaccessible under section 21, shall, at the time of the execution of the Search and Seizure Warrant, or as soon as practicable thereafter–

(a) make a list of the seized or rendered computer system, with the date and time of seizure or rendering; and

(b) submit a copy of the list to–

(i) the person to whom the warrant is addressed; or

(ii) the occupier of the premises at which the warrant is executed.

(2) A person, who immediately before the execution of a warrant, had possession or control of a computer system or a computer data storage medium seized, may request a copy of computer data from the police officer who executed the Search and Seizure Warrant, and the police officer shall, as soon as is reasonably practicable, comply with the request.

(3) Notwithstanding sub-section (2), a police officer who seizes a computer system or computer data storage medium may refuse to provide a copy of computer data if the police officer has reasonable grounds for believing that providing the copy would–

(a) constitute or facilitate the commission of a criminal offence; or

(b) prejudice–

(i) the investigation in relation to the Search and Seizure Warrant;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation mentioned in sub-paragraph *(i)* or *(ii).*

Assistance.

25.–(1) A person with knowledge about the functioning of a computer system or computer data storage medium, or security measures applied to protect computer data, that is the subject of a Search and Seizure Warrant shall, if requested, assist the police officer who is executing the search, by–

(a) providing any information, about the computer system, computer data or storage medium sought, that may facilitate the execution of the Search and Seizure Warrant;

(b) accessing and using the computer system or computer data storage medium to search computer data which is stored in, or lawfully accessible from or available to, that computer system or computer data storage medium;

(c) obtaining and copying computer data; or

(d) obtaining an intelligible output from a computer system or computer data storage medium in such a format that is admissible for the purpose of legal proceedings.

(2) A person who fails, without lawful excuse or justification, to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for one year.

Ex-parte application for Production Order.

26.–(1) The Director of Public Prosecutions or Head Prosecution Branch may, in the prescribed form, make an *ex-parte* application to the Court for a Production Order.

(2) An application under sub-section (1), shall be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(a) the name of the investigating police officer;

(b) the facts or allegations giving rise to the application, including the alleged offence;

(c) full particulars of all facts and circumstances alleged by the applicant, including–

(i) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the application relates; and

(ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained if the Production Order is granted;

(d) where applicable–

(i) whether other investigative procedures were applied and whether they failed to produce the required evidence; or

(ii) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(iii) the requested duration of the Order;

(iv) whether any previous application was made for a Production Order in respect of the same person, facility or premises, and the status of that other application; and

(v) any other relevant directives issued by a Court in relation to the matter.

(3) A Court shall issue a Production Order, where it is satisfied that computer data or traffic data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law.

(4) A Production Order may direct–

(a) a person in Belize who is in possession or control of a computer system or computer data storage medium, to produce, from the computer system or computer data storage medium, specified computer data or a printout or other intelligible output of the computer data; or

(b) a service provider in Belize to produce traffic data relating to information transmitted from a subscriber through a computer system or from other relevant persons, or subscriber information about a person who uses the service, and give it to a specified person within a specified period.

Expedited Preservation Order.

27.–(1) A Judge, if satisfied on an *ex-parte* application by the Director of Public Prosecution, or a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that computer data or traffic data that is reasonably required for the purpose of a criminal investigation, under this Act or any other law, is vulnerable to loss or modification, may make an order requiring a person in possession or control of computer data or traffic data to preserve and maintain the integrity of the computer data or traffic data for a period not exceeding ninety days.

(2) A Judge, on an *ex-parte* application by the Director of Public Prosecution or a police officer of the rank of Superintendent or above, may order an extension of the period referred to in subsection (1) by a further specified period of ninety days or more but not exceeding one year on a special case by case basis.

Removal or Disablement of Data Order.

28.–(1) The Director of Public Prosecutions or police officer, the rank of superintendent or above may, in the prescribed form, make an *ex-parte* application to the Court for a Removal or Disablement Order.

(2) Where on an application under sub-section (1), the Court is satisfied that a service provider or other entity within a domain name server is deleting, modifying, suppressing, storing, transmitting or providing access to computer data in contravention of this Act or any other law, the Court may order the service provider or entity to remove or disable access to the computer data.

Ex-parte application for Remote Forensic Tools Order.

29.–(1) The Director of Public Prosecutions may, in the prescribed form, make an *ex-parte* application to the Court for a Use of Remote Forensic Tools Order.

(2) An application under sub-section (1), shall be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(a) the basis for the application, including that it is the interest of–

(i) national security

(ii) public safety;

(iii) public health;

(iv) public order;

(v) child luring or pornography;

(vi) human trafficking;

(vii) slavery; or

(viii) giving effect to the requirements of a mutual legal assistance request where the alleged offence is an offence under the laws of Belize.

(b) the name, and where possible, the address, of the person who is suspected of committing the alleged offence;

(c) a description of the targeted computer system;

(d) a description of the required tool, the extent and duration of its utilisation; and

(e) the reason for the use of the tool.

(3) A Court shall issue a Use of Remote Forensic Tools Order, where it is satisfied that computer data that is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law cannot be collected without the use of the Use of Remote Forensic Tools Order.

(4) On an application under subsection (1), the Court may order that a person or a service provider support the installation of the remote forensic tool.

(5) A Use of Remote Forensic Tools Order shall be in relation to the following only–

(a) modifications to a computer system shall be limited to those that are necessary for the investigation; and

(b) modification to a computer system shall be done, so far as possible, after the investigation.

(6) A police officer who executes a Use of Remote Forensic Tools Order as soon as possible after execution, prepare a record of–

(a) the remote forensic tool used;

(b) the time and date the remote forensic tool was used;

(c) the identification of the computer system and details of the modification undertaken; and

(d) the information obtained.

(7) A police officer who executes a Use of Remote Forensic Tools Order shall ensure that any information obtained by the utilisation of the remote forensic tool is protected against modification, unauthorised deletion and unauthorised access.

(8) A Use of Remote Forensic Tools Order shall cease to apply where–

(a) the computer data sought is collected;

(b) there is no longer any reasonable ground for believing that the computer data sought exists; or

(c) the conditions of the authorisation are no longer present.

(9) For the purposes of this section, “remote forensic tool” means an investigative software or hardware installed on or attached to a computer system that is used to perform a task.

Offence to disclose confidential information.

30.–(1) A person who is the subject of an Order under this Act shall not disclose to any other person–

(a) the fact that an Order was made;

(b) the details of the Order;

(c) anything done pursuant to the Order; or

(d) any compute or traffic data, subscriber information or other information collected or recorded pursuant to the Order under this Act.

(2) Sub-section (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting an alleged offender.

(3) A person who without lawful excuse or justification, fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years.

No liability for person aiding in enforcement of Act.

31. A person or service provider shall not be liable for any actions taken or the disclosure of any computer data or other information that may be disclosed pursuant to the enforcement of this Act.

Application for Compensation Order.

32.–(1) A person who believes that they have suffered loss or damage due to the commission of an offence under this Act, may make an application for a Compensation Order.

(2) The Court may make an order under sub-section (1) of its own motion.

(3) A Court shall, where it is satisfied on an application under sub-section (1), that the applicant has suffered pain and suffering, loss, harm or injury, that is caused by the commission of an offence under this Act, grant the Compensation Order.

(4) A Compensation Order under sub-section (1) shall be without prejudice to any other remedy which the applicant has under any other law.

(5) An application under sub-section (1) shall be made prior to sentencing of the person against whom the Compensation Order is sought and be in accordance with rules of Court.

Ex-parte application for Forfeiture Order and issue of Restraint Order.

33.–(1) Subject to sub-section (2), where a person is convicted of an offence under this Act, the court that heard the criminal case may, upon the application of the Director of Public Prosecutions, order that any property–

(a) used for or in connection with; or

(b) obtained as a result of or in connection with, the commission of the offence

be forfeited to the State.

(2) Before making a Forfeiture Order, the Court shall give an opportunity to be heard to any person who–

(a) claims to be the owner of the property that is the subject of the Order; or

(b) appears to the Court to have an interest in the property that is the subject of the Order.

(3) Where the Court is satisfied that the requirements under sub-section (2) have been met, the Court shall grant the Forfeiture Order and issue–

(a) a warrant authorising a police officer to search the building, place or vessel for the property that is the subject of the Forfeiture Order and to seize–

(i) the property if found; and

(ii) any other property in respect of which the police officer has reasonable grounds to believe that the Forfeiture Order under ought to have been made; or

(b) a Restraint Order prohibiting any person from disposing of, or otherwise dealing with any interest in, the property, other than as specified in the Restraint Order.

(4) A person against whose property an Order under this section is made, may appeal the Order.

(5) Property forfeited to the State under sub-section (1) shall vest in the State–

(a) if no appeal is made against the Forfeiture Order, within the period for an appeal; or

(b) if an appeal is made, on the final determination of the matter, where the decision is made in favour of the State.

Failure to comply with a Court Order.

34. A person who fails to comply with any Order of the Court, under this Act, commits an offence and is liable–

(a) to a fine of one thousand dollars and to a term of imprisonment for one year; and

(b) where applicable, to a further daily fine for each day the offence continues, of not more than fifty thousand dollars until the relevant corrective action has been taken.

Evidence.

35. In any criminal proceedings under this Act or any other law–

(a) any computer data or traffic data, generated, retrieved or reproduced from a computer system, and whether in electronic or printed form; or

(b) any computer acquired in respect of any offence,

shall be admissible as evidence.

Determining the severity of charges.

36. It shall be within the discretion of the Director of Public Prosecutions to determine whether an offence is tried summarily or on indictment.

PART IV

International Cooperation

Mutual Legal Assistance Act No. 8 of 2014.

37. For the purposes of international cooperation, the Mutual Legal Assistance Act shall apply.

Spontaneous information**.**

38.–(1) The Central Authority may, concerning the possible commission of any offence under this Act, and without prior request, forward to foreign government or international agency information obtained within the framework of an investigation when it considers that the disclosure of the information might assist the foreign government or international agency in initiating or carrying out investigations or proceedings concerning criminal offences under its own law or applicable laws or might lead to a request for mutual legal assistance under this Act.

(2) The Central Authority may request that the information provided under sub-section (1) be kept confidential or only used subject to conditions.

(3) Where the information provided cannot kept confidential, the Central Authority may determine if the spontaneous information should be shared.

Extradition.

CAP. 112.

39. The offences described in this Act shall be deemed to be extraditable offences and the Extradition Act shall apply.

Transborder access to computer data with consent or when unsecured and publicly available.

40. It shall not be an offence under this Act for any foreign government or any person to, without the authorisation of the Government of Belize or any person–

(a) access open source stored computer data, regardless of where the data is located, if the computer data is not subjected to security measures; or

(b) access or receive stored computer data located in Belize, if the foreign government or person obtains the consent of the person who has the authority to disclose the data through that computer system.

PART V

Miscellaneous

Use of computer system to commit offence under other law.

41. Where an offence, under any other law, is committed through the use of a computer system, the offender is liable on conviction to a fine of four times the penalty stated in the other law.

Corporate liability.

42. –(1) Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence.

(2) Where a body corporate commits an offence under this Act and the Court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate–

(a) consented or connived in the commission of the offence; or

(b) failed to exercise due diligence to prevent the commission of the offence,

that director, manager, secretary, or other similar officer commits an offence.

(3) A person who commits an offence under sub-section (2) is liable on–

(a) summary conviction to a fine of five thousand dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of eight thousand dollars and to imprisonment for five years.

Jurisdiction.

43. A Court in Belize shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out–

(a) wholly or in substantial part within its territory;

(b) against the status of persons, or interests in things, present within its territory;

(c) outside its territory but has or is intended to have substantial effect within its territory;

(d) against the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(e) outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

Regulations.

44. The Minister may make regulations prescribing all matters that are required to be prescribed under this Act and for such other matters as may be necessary for giving full effect to this Act and for its proper administration.