THE CYBERCRIME BILL, 2017

Explanatory Notes

(These notes form no part of the Bill but are intended only to indicate its general purport)

The purpose of the Cybercrime Bill, 2017 is to provide for the creation of offences related to cybercrime and for other related matters in Trinidad and Tobago. The Bill would be inconsistent with sections 4 and 5 of the Constitution and is therefore required to be passed by a special majority of three-fifths of the members of each House.

Part I of the Bill would provide for certain preliminary matters.

Clause 1 provides for the short title.

Clause 2 would provide for the Act to come into operation on Proclamation by the President.

Clause 3 provides that the Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution.

Clause 4 would define certain terms used in the Bill.

Part II of the Bill would create certain offences related to cybercrime.

Clause 5 seeks to create the offence of illegally accessing a computer system. This offence would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

Clause 6 seeks to create the offence of illegally remaining in a computer system which would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of two hundred thousand dollars and three years' imprisonment on conviction on indictment.

Clause 7 seeks to create the offence of illegally interfering with computer data and would include damaging or deleting computer data. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a

fine of two hundred thousand dollars and three years' imprisonment on conviction on indictment.

Clause 8 seeks to create the offence of illegally acquiring computer data. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of five hundred thousand dollars and three years' imprisonment on conviction on indictment. This clause also seeks to create the offence of receiving or gaining access to computer data knowing that it is obtained illegally, and would carry the same penalty as that of the offence of illegally acquiring computer data.

Clause 9 seeks to create the offence of illegally interfering with a computer system or with a person who is using or operating a computer system. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of three hundred thousand dollars and three years' imprisonment on conviction on indictment.

Clause 10 seeks to impose greater penalties on persons who commits an offence under Part II and which affects critical infrastructure. This clause would define "critical infrastructure" as any computer system, device, network, computer program or computer data so vital to the State that the incapacity or destruction of, or interference with, such system, device, network, program or data would have a debilitating impact on the security, defence or international relations of the State or the provision of services directly related to national or economic security, banking and financial services, public utilities, the energy sector, communications infrastructure, public transportation, public health and safety, or public key infrastructure. An offence under this clause would carry a penalty of two million dollars and fifteen years' imprisonment on conviction on indictment.

Clause 11 seeks to create the offence of illegally producing, selling, procuring, importing, exporting, distributing or otherwise making available a computer device or program for the purpose of committing an offence under the Act. This offence would carry a fine of two hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

Clause 12 seeks to create the offence of the unauthorized grant of access to computer data that is commercially sensitive or a trade

secret, which relates to the national security of the State, or which is stored on a computer system and is protected against unauthorized access. This offence would carry a fine of two hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

Clause 13 seeks to create the offence of computer-related forgery. This would make it unlawful to input, alter, delete or suppress computer data which would result in inauthentic data and would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment. This clause would also provide for the commission of the offence of computer-related forgery by sending out multiple electronic mail messages and would carry an additional fine of two hundred thousand dollars and three years' imprisonment.

Clause 14 seeks to create the offence of computer-related fraud which causes loss of, or damage to property and would carry a fine of one million dollars and five years' imprisonment on summary conviction or a fine of two million dollars and ten years' imprisonment on conviction on indictment.

Clause 15 seeks to create the offence of identity theft through the use of a computer system which would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

Clause 16 seeks to create the offence of violating a person's privacy by capturing and sharing pictures or videos of a person's private area without his consent. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of five hundred thousand dollars and three years' imprisonment on conviction on indictment.

Clause 17 seeks to criminalise the act of sending electronic mail messages which cause damage to a computer system. This offence would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

Clause 18 seeks to create the offence of causing harm to a person through communication via a computer system. This offence would carry a fine of one hundred thousand dollars and three years' imprisonment on summary conviction or a fine of two hundred and fifty thousand dollars and five years' imprisonment on conviction on indictment. This clause would also provide factors that a Court may take into consideration in determining whether an offence is committed under the section.

Clause 19 would create the offence of using a computer system to extort a benefit from another person. This offence would carry a fine of one hundred thousand dollars and three years' imprisonment on summary conviction or a fine of two hundred and fifty thousand dollars and five years' imprisonment on conviction on indictment.

Part III of the Bill provides for certain enforcement provisions.

Clause 20 would provide for the jurisdiction of the Courts of Trinidad and Tobago as it would relate to its territorial limits under the Act.

Clause 21 would empower the Court to authorize the search and seizure of apparatus and computer data necessary for establishing an offence or which has been acquired by a person as a result of the commission of an offence.

Clause 22 would impose liability on a person who has knowledge about the functioning of a computer system but who fails to render assistance to access computer data that is the subject of a search warrant.

Clause 23 would empower a Magistrate to order an internet service provider or any entity with a domain name server to remove or disable computer data that is being stored or transmitted in contravention of the Act.

Clause 24 would empower the Court to make a production order relating to computer data that is required for a criminal investigation or criminal proceedings.

Clause 25 empowers a Magistrate to order the expedited preservation of computer data if he has reasonable grounds to believe that the data is susceptible to modifications.

Clause 26 would impose liability on an internet service provider who intentionally and without lawful excuse discloses the details of an Order of a Court.

Clause 27 would give authority to a Magistrate, who has reasonable grounds to believe that data stored in a computer system is required for a criminal investigation, to order the partial disclosure of traffic data.

Clause 28 would provide that a Magistrate may authorize a police officer to utilize remote forensic tools if he reasonably believes that evidence cannot be collected without the use of such tools. The Schedule to the Act would stipulate the offences for which these tools may be used.

Clause 29 would empower the Court to order payment of an additional fine where monetary benefits were gained as a result of the commission of an offence under the Act or where loss or damage was caused as a result.

Clause 30 would empower the Court to order payment of compensation for loss or damage suffered as a penalty for offences under the Act and the procedure for making an application for such compensation.

Clause 31 would provide the procedure for the Court to make a forfeiture order and the treatment of property forfeited as it relates to any property used for, or in connection with, or obtained as proceeds from the commission of an offence under the Act.

Clause 32 would empower the Court to issue a warrant for the search and seizure, and a restraint order to prohibit the disposal of, any property that is to be forfeited under the Act.

Part IV of the Bill seeks to make provisions related to internet service providers.

Clause 33 would provide that an internet service provider is not under an obligation to monitor the information which it transmits or stores on behalf of another person or to actively seek facts or circumstances which would indicate illegal activity. This clause also seeks to prohibit an internet service provider from refusing to comply with any order of the Court or other legal requirement.

Clause 34 would provide that an access provider is not criminally liable for providing access to, or transmitting information prohibited by the Act under certain circumstances.

Clause 35 would provide that a hosting provider is not criminally liable for the storage of information prohibited by the Act under certain circumstances.

Clause 36 would provide that a caching provider is not criminally liable for storing information prohibited by the Act under certain circumstances.

Clause 37 would provide that an internet service provider is not criminally liable for enabling access, via electronic hyperlink, to information provided by another person in contravention of the Act under certain circumstances.

Clause 38 would provide that a search engine provider who creates an index of internet-related content or makes available electronic tools to search for information is not criminally liable if he does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission.

Part V of the Bill provides for certain miscellaneous provisions.

Clause 39 would give the Minister the power to make Regulations for the proper administration of the Act.

Clause 40 would require the Minister to cause the Act to be reviewed at least once every three years after it comes into force.

Clause 41 would repeal the Computer Misuse Act, Chap. 11:17.

THE CYBERCRIME BILL, 2017

ARRANGEMENT OF CLAUSES

PART I

PRELIMINARY

PART II

CYBERCRIME OFFENCES

PART III

ENFORCEMENT

A BILL

An Act to provide for the creation of offences related to cybercrime and related matters

WHEREAS it is enacted by section 13(1) of the Constitution that an Act of Parliament to which that section applies may expressly declare that it shall have effect even though inconsistent with sections 4 and 5 of the Constitution and, if any Act does so declare, it shall have effect accordingly:

And whereas it is provided in section 13(2) of the Constitution that an Act of Parliament to which that section applies is one the Bill for which has been passed by both Houses of Parliament and at the final vote thereon in each House has been supported by the votes of not less than three-fifths of all the members of that House:

And whereas it is necessary and expedient that the provisions of this Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution:

ENACTED by the Parliament of Trinidad and Tobago as follows: Enactment

PART I

PRELIMINARY

1. This Act may be cited as the Cybercrime Act, 2017. Short title

2. This Act comes into operation on such date as is fixed by the President by Proclamation. Commencement

3. This Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution. Act inconsistent with Constitution

4. In this Act – Interpretation

"computer data" means any representation of –

(a) facts;

(b) concepts;

(c) machine-readable code or instructions; or

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

that is in a form suitable for processing in a computer system and is capable of being sent, received or stored, and includes a program that can cause a computer system to perform a function;

"computer data storage medium" means anything in which information is capable of being stored, or anything from which information is capable of being retrieved or reproduced, with or without the aid of any other article or device;

"computer program" or "program" means 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 program or external instruction to perform automatic processing of information or electronic data;

Act No. 6 of 2011

"data message" has the meaning assigned to it in the Electronic Transactions Act;

"device" means any electronic programmable device used, whether by itself or as part of a computer network, an electronic communications network or any other device or equipment, or any part thereof, to perform pre-determined arithmetic, logical, routing or storage operations and includes –

(a) an input device;
(b) an output device;
(c) a processing device;
(d) a computer data storage medium;
(e) a program; or
(f) equipment,

that is related to, connected with or used with such a device or any part thereof;

"electronic mail message" means an unsolicited data message, including electronic mail and an instant message;

"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;

"hinder" in relation to a computer system, includes –

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

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system; or

(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

"internet service provider" includes a person who provides the services referred to in Part IV;

"Minister" means the minister to whom responsibility for national security is assigned;

"remote forensic tools" means investigative software or hardware installed on or attached to a computer system that is used to perform a task that includes keystroke logging or transmission of an internet protocol address;

"traffic data" means computer data that –

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services,

and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

PART II

CYBERCRIME OFFENCES

Illegal access to a computer system

5. A person who, intentionally and without lawful excuse or justification, accesses a computer system or any part of a computer system, commits an offence and is liable –

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

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

Illegally remaining in a computer system

6. A person who, intentionally and without lawful excuse or justification, remains logged into a computer system or part of a computer system or continues to use a computer system commits an offence and is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or

(b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years.

Illegal data interference

7. (1) A person who, intentionally and without lawful excuse or justification –

(a) damages computer data or causes computer data to deteriorate;

(b) deletes computer data;

(c) alters computer data;

(d) copies computer data to any computer data storage device or to a different location within the computer system;

(e) moves computer data to a computer storage device or a different location within the computer system;

(f) renders computer data meaningless, useless or ineffective;

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

(h) obstructs, interrupts or interferes with a person in his lawful use of computer data; or

(i) denies access to computer data to a person who is authorised to access it,

commits an offence.

(2) A person who commits an offence under subsection (1), is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or

(b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years.

Illegal acquisition of data

8. (1) A person who intentionally and without lawful excuse or justification accesses a computer system without

authorisation, or by exceeding authorised access, and obtains computer data commits an offence and is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or

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

(2) A person who intentionally and without lawful excuse or justification receives or gains access to computer data knowing the same to have been stolen or obtained pursuant to sub-section (1) commits an offence and is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or

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

Illegal system interference

9. (1) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a computer system commits an offence.

(2) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a person who is lawfully using or operating a computer system commits an offence.

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

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or

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

Offences affecting critical infrastructure

10. (1) Notwithstanding the penalties set out in sections 5 to 9, where a person commits an offence under any of those sections and the offence results in hindering, or interference with, a computer system that –

(a) is exclusively for the use of critical infrastructure; or

(b) affects the use, or impacts the operation, of critical infrastructure,

he is liable on conviction on indictment to a fine of two million dollars and imprisonment for fifteen years.

(2) For the purpose of this section, "critical infrastructure" means any computer system, device, network, computer program or computer data so vital to the State that the incapacity or destruction of, or interference with, such system, device, network, program or data would have a debilitating impact on the –

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

(b) provision of services directly related to national or economic security, banking and financial services, public utilities, the energy sector, communications infrastructure, public transportation, public health and safety, or public key infrastructure.

Illegal devices

11. (1) A person who –

(a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available or has in his possession –

(i) a device, or computer program, that is designed or adapted for the purpose of committing an offence under this Act; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data is capable of being accessed,

with the intent that it be used for the purpose of committing an offence under this Act; or

(b) intentionally and without lawful excuse or justification discloses a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data can be accessed -

(i) for unlawful gain, whether for himself or another person;

(ii) for an unlawful purpose; or

(iii) knowing that it is likely to cause unlawful damage,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable –

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

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

Unauthorised granting of access to computer data

12. (1) A person who, through authorised or unauthorised means, obtains or accesses computer data which –

(a) is commercially sensitive or a trade secret;

(b) relates to the national security of the State; or

(c) is stored on a computer system and is protected against unauthorized access,

and intentionally and without lawful excuse or justification grants access to or gives the computer data to another person, whether or not he knows that the other person is authorised to receive or have access to the computer data, commits an offence.

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

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

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

Computer-related forgery

13. (1) A person who, intentionally and without lawful excuse or justification inputs, alters, deletes or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon as if it were authentic, regardless of whether or not the data is directly readable and intelligible, commits an offence and is liable –

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

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

(2) A person who commits an offence under subsection (1) by sending out multiple electronic mail messages from or through a computer system, is liable on conviction to a fine of two hundred thousand dollars and imprisonment for three years, in addition to the penalty set out in subsection (1).

Computer-related fraud

14. (1) A person who, intentionally and without lawful excuse or justification –

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

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

with the intent of procuring an economic benefit for himself or another person and thereby causes loss of, or damage to, property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of one million dollars and imprisonment for five years; or

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

Identity-related offences

15. A person who intentionally transfers, possesses or uses a means of identification, other than his own, with the intent of committing an unlawful act through the use of a computer system, commits an offence and is liable –

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

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

Violation of privacy

16. (1) A person who intentionally and without lawful excuse or justification –

(a) captures; or

(b) stores in, or publishes or transmits through a computer system,

the image of the private area of another person without his consent, where the other person has a reasonable expectation that he could disrobe in privacy, or that his private area would not be visible to the public regardless of whether he is in a public or private place,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; and

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

(3) For the purposes of this section, "private area" means the genitals, pubic area, buttocks or breast.

Causing damage by electronic mail message

17. (1) A person who maliciously initiates, relays or re-transmits an electronic mail message from or through a computer system and thereby causes damage to a computer system commits an offence.

(2) A person who intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under subsection (1) commits an offence.

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

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

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

Causing harm by communication using a computer system

18. (1) A person who uses a computer system to communicate with the intention to cause harm to another person commits an offence.

(2) In determining whether an offence is committed under this section, the Court may take into account any factor which it considers relevant, including –

(a) the extremity of the language used in the communication;

(b) the age and characteristics of the person involved;

(c) whether the communication was anonymous;

(d) whether the communication was repeated;
(e) the extent of circulation of the communication;
(f) whether the communication is true or false; and
(g) the context in which the communication appeared.

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

(a) on summary conviction to a fine of one hundred thousand dollars and to imprisonment for three years; and
(b) on conviction on indictment to a fine of two hundred and fifty thousand dollars and imprisonment for five years.

(4) For the purposes of this section, "harm" means serious emotional distress.

Intent to extort a benefit

19. A person who uses a computer system with the intent to extort a benefit from another person by threatening to publish computer data containing personal or private information which can cause public ridicule, contempt, hatred or embarrassment commits an offence and is liable –

(a) on summary conviction to a fine of one hundred thousand dollars and to imprisonment for three years; and
(b) on conviction on indictment to a fine of two hundred and fifty thousand dollars and imprisonment for five years.

PART III

ENFORCEMENT

Jurisdiction

20. (1) A Court in Trinidad and Tobago shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out –

(a) wholly or partly in Trinidad and Tobago;
(b) by a citizen of Trinidad and Tobago, whether in Trinidad and Tobago or elsewhere; or
(c) by a person on board a vessel or aircraft registered in Trinidad and Tobago.

(2) For the purpose of subsection (1)(a), an act is carried out in Trinidad and Tobago if –

(a) the person is in Trinidad and Tobago at the time when the act is committed;

(b) a computer system located in Trinidad and Tobago or computer data on a computer data storage device located in Trinidad and Tobago is affected by the act; or

(c) the effect of the act, or the damage resulting from the act, occurs within Trinidad and Tobago.

(3) Subject to subsection (1), a Summary Court has jurisdiction to hear and determine any offence under this Act, if –

(a) the accused was within the magisterial district at the time when he committed the offence;

(b) a computer system, containing any computer program or computer data which the accused used, was within the magisterial district at the time when he committed the offence; or

(c) damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies.

Search and seizure

21. (1) Where a Magistrate is satisfied on the basis of information on oath by a police officer that there is reasonable ground to believe that there is in a place an apparatus or computer data –

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

(b) that has been acquired by a person as a result of an offence under this Act,

he may issue a warrant authorizing a police officer, with such assistance as may be necessary, to enter the place to search for and seize the apparatus or computer data.

(2) If a police officer who is undertaking a search under this section has reasonable grounds to believe that –

(a) the computer data sought is stored in another apparatus; or

(b) part of the computer data sought is in another place within Trinidad and Tobago,

and such computer data is lawfully accessible from, or available to the first apparatus, he may extend the search and seizure to that other apparatus or other place.

(3) In the execution of a warrant under this section, a police officer may, in addition to the powers conferred on him by the warrant –

(a) activate an onsite computer system or computer data storage media;
(b) make and retain a copy of computer data;
(c) remove computer data in a computer system or render it inaccessible;
(d) take a printout of the output of computer data;
(e) impound or similarly secure a computer system or part of it or a computer data storage medium; or
(f) remove a computer system or computer data storage medium from its location.

(4) A police officer who undertakes a search under this section shall secure any apparatus and maintain the integrity of any computer data that is seized.

(5) For the purpose of this section, "apparatus" includes –

(a) a computer system or part of a computer system; or
(b) a computer data storage medium.

Assistance

22. (1) A person who has knowledge about the functioning of an apparatus, or measures applied to protect computer data, that is the subject of a search warrant shall, if requested by the police officer authorised to undertake the search, assist the officer by –

(a) providing information that facilitates the undertaking of the search for and seizure of the apparatus or computer data sought;
(b) accessing and using an apparatus to search computer data which is stored in, or lawfully accessible from, or available to, that apparatus;

(c) obtaining and copying computer data; or

(d) obtaining an intelligible output from an apparatus in such a format that is admissible for the purpose of legal proceedings.

(2) A person who fails to comply with this section commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and imprisonment for one year.

Order for removal or disablement of data

23. If a Magistrate is satisfied on the basis of information on oath by a police officer that an internet service provider or any other entity with a domain name server is storing, transmitting or providing access to information in contravention of this Act or any other written law, the Magistrate may order the internet service provider or other entity with a domain name server to remove, or disable access to, the information.

Production Order

24. If a Magistrate is satisfied on the basis of information on oath by a police officer that computer data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Magistrate may order –

(a) a person in Trinidad and Tobago who is in control of an apparatus, to produce from the apparatus computer data or a printout or other intelligible output of the computer data; or

(b) an internet service provider in Trinidad and Tobago to produce information about a person who subscribes to, or otherwise uses his service.

Expedited preservation

25. (1) A Magistrate may, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above, that there are grounds to believe that computer data that is reasonably required for the purpose of a criminal investigation is vulnerable to loss or modification, authorise the police officer to require a person in control of the computer data, by notice in writing, to preserve the data for such period not exceeding ninety days as is stated in the notice.

(2) A Magistrate may, on an *ex parte* application by a police officer of the rank of Superintendent or above, authorise an extension of the period referred to in subsection (1) by a further specified period not exceeding ninety days.

Disclosure of details of an order

26. (1) If an order under section 24 or a notice under section 25 stipulates that confidentiality is to be maintained, a person who is the subject of the order or notice and who intentionally and without lawful excuse or justification discloses –

(a) the fact that the order or notice has been made;

(b) the details of the order or notice;

(c) anything done pursuant to the order or notice; or

(d) any data collected or recorded pursuant to the order,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable –

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

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

Disclosure of traffic data

27. If a Magistrate is satisfied on the basis of information on oath by a police officer, that there are reasonable grounds to believe that computer data stored in an apparatus is reasonably required for the purpose of a criminal investigation into a data message, he may require a person to disclose sufficient traffic data about the data message to identify –

(a) the internet service provider; or

(b) the path,

through which the data message was transmitted.

Remote forensic tools

Schedule

28. (1) If a Judge is satisfied on *ex parte* application by a police officer, that there are reasonable grounds to believe that computer data which is required for the purpose of a criminal investigation into an offence listed in the Schedule cannot be collected without the use of a remote forensic tool, the Judge may authorise a police officer, with such assistance as may be necessary, to utilise such tool for the investigation.

(2) An application made under subsection (1) shall contain the following information:

(a) the name, and if possible, the address of the person who is suspected of committing the offence;

(b) a description of the targeted computer system;
(c) a description of the required tool, and the extent and duration of its utilization; and
(d) reason for the use of the tool.

(3) Where an application is made under subsection (1), the Judge may order that an internet service provider support the installation of the remote forensic tool.

(4) Where a remote forensic tool is utilised under this section –

(a) modifications to a computer system shall be limited to those that are necessary for the investigation;
(b) modifications to a computer system shall be undone, so far as possible, after the investigation; and
(c) the following information shall be logged:
  (i) the technical means used;
  (ii) the time and date of the application;
  (iii) the identification of the computer system and details of the modification undertaken; and
  (iv) the information obtained.

(5) The police officer responsible for a criminal investigation in which a remote forensic tool is utilised under this section shall ensure that any information obtained by the utilisation of the remote forensic tool is protected against modification, unauthorised deletion and unauthorised access.

(6) An authorization that is granted under this section 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 authorization are no longer present.

(7) The Minister may, by Order, amend the Schedule.

(8) For the purpose of this section, "utilise" includes –

(a) accessing a computer system;

(b) developing a remote forensic tool;

(c) adopting a remote forensic tool; or

(d) acquiring a remote forensic tool.

Order for payment of additional fine

29. (1) Where a person is convicted of an offence under this Act and the Court is satisfied that monetary benefits accrued to him as a result of the commission of the offence, the Court may order him to pay an additional fine in an amount equal to the amount of the monetary benefits.

(2) Where damage is caused as a result of an offence under this Act, the person convicted of the offence is liable to an additional fine not exceeding the fine that the Court may impose for the commission of the offence that caused the damage.

Order for payment of compensation

30. (1) Where a person is convicted of an offence under this Act, and the Court is satisfied that another person has suffered loss or damage because of the commission of the offence, it may, in addition to any penalty imposed under this Act, order the person convicted to pay a fixed sum as compensation to that other person for the loss or damage caused or likely to be caused, as a result of the commission of the offence.

(2) An order made under subsection (1) shall be without prejudice to any other remedy which the person who suffered the damage may have under any other law.

(3) The Court may make an order under this section of its own motion or upon application of a person who has suffered damage as a result of the commission of the offence.

(4) A person who makes an application under subsection (3) shall do so before sentence is passed on the person against whom the order is sought.

(5) For the purpose of this section, computer data held in an apparatus is deemed to be the property of the owner of the apparatus.

Forfeiture Order

31. (1) Subject to subsection (2), where a person is convicted of an offence under this Act, the Court may 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 an order under subsection (1), the Court shall give an opportunity to be heard to any person who claims to be the owner of the property or who appears to the Court to have an interest in the property.

(3) Property forfeited to the State under subsection (1) shall vest in the State—

(a) if no appeal is made against the order, at the end of the period within which an appeal may be made against the order; or

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

(4) Where property is forfeited to the State under this section, it shall be disposed of in the prescribed manner.

Order for seizure and restraint

32. Where an *ex parte* application is made by the Director of Public Prosecutions to a Judge and the Judge is satisfied that there are reasonable grounds to believe that there is in any building, place or vessel, any property in respect of which a forfeiture order under section 31 has been made, the Judge may issue –

(a) a warrant authorising a police officer to search the building, place or vessel for that property and to seize that property if found, and any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 31 may be made; or

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

PART IV

INTERNET SERVICE PROVIDERS

No monitoring obligation

33. (1) Subject to subsection (2), an internet service provider who provides a conduit for the transmission of information, shall not be responsible for –

(a) monitoring the information which he transmits or stores on behalf of another in order to ascertain whether its processing would constitute or give rise to liability under this Act; or

(b) actively seeking facts or circumstances indicating illegal activity in order to avoid criminal liability under this Act.

(2) Subsection (1) does not relieve an internet service provider from complying with any court order, injunction, writ or other legal requirement, which obliges an internet service provider to terminate or prevent an infringement based on any written law.

Access provider

34. (1) An access provider shall not be liable under this Act for providing access and transmitting information if he does not –

(a) initiate the transmission;

(b) select the receiver of the transmission; or

(c) select or modify the information contained in the transmission.

(2) For the purpose of this section –

"access provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by transmitting information provided by, or to a user of the service in a communication network or provides access to a communication network;

"communication network" means a set of devices or nodes connected by communication links, which is used to provide the transfer of computer data between users located at various points or other similar services; and

"transmit" or "provide access" includes the automatic, intermediate and transient storage of information transmitted in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a

period longer than is reasonably necessary for the transmission.

Hosting provider

35. (1) A hosting provider shall not be liable for the storage of information in contravention of this Act if –

(a) he expeditiously removes or disables access to the information after receiving a lawful order from any appropriate authority to remove specific illegal information stored; or

(b) upon obtaining knowledge or awareness, by ways other than a lawful order from any appropriate authority, about specific illegal information stored, he expeditiously informs the authority to enable it to evaluate the nature of the information and, if necessary, issue an order to remove the content.

(2) This section shall not apply when the user of the service is acting under the authority or control of the hosting provider.

(3) For the purpose of this section –

"hosting provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by storing information provided by a user of his service.

Caching provider

36. (1) A caching provider shall not be liable for the storage of information in contravention of this Act if –

(a) he does not modify the stored information;

(b) he complies with the condition of access to the stored information;

(c) he updates stored information in accordance with any written law or in a manner that is widely recognised and used in the information communication technology industry; or

(d) he does not interfere with the lawful use of technology, widely recognised and used by the information communication

technology industry, to obtain data on the use of the stored information,

and acts expeditiously to remove or to disable access to the information he has stored upon obtaining knowledge of the fact that –

(e) the stored information at the initial source of the transmission has been removed from the network;

(f) access to the stored information has been disabled; or

(g) a Court has ordered the removal or disablement of the stored information.

(2) For the purpose of this section –

"caching provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by the automatic, intermediate and temporary storage of information, where such storage is for the sole purpose of making the onward transmission of the information to other users of the service more efficient.

Hyperlink provider

37. (1) An internet service provider who enables the access to information provided by another person, by providing an electronic hyperlink, shall not be liable for information that is in contravention of this Act if –

(a) the internet service provider expeditiously removes or disables access to the information after receiving a lawful order from any appropriate authority to remove the link; or

(b) the internet service provider, upon obtaining knowledge or awareness, by ways other than a lawful order from any appropriate authority, expeditiously informs the authority to enable it to evaluate the nature of the information and if necessary issue an order to remove the content.

(2) For the purpose of this section –

"hyperlink" means a characteristic or property of an element such as a symbol, word,

phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.

Search engine provider

38. A provider who makes or operates a search engine that either automatically, or based on entries by others, creates an index of internet-related content or, makes available electronic tools to search for information provided by another person, shall not be liable under this Act for the search results if the provider –

(a) does not initiate the transmission; or

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

PART V
MISCELLANEOUS

Regulations

39. (1) 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.

(2) Regulations made under this section shall be subject to negative resolution of Parliament.

Review of the Act

40. The Minister shall cause the Act to be reviewed at least once every three years from the date on which it comes into operation.

Repeal of Chap. 11:17

41. The Computer Misuse Act is repealed.

SCHEDULE

[Section 28]

OFFENCES

1. Offences involving treason under the Treason Act, Chap. 11:03
2. Offences against the person, namely –
   (a) Murder
   (b) Manslaughter

3. Offences involving kidnapping
4. Drug trafficking, namely –
    (a) Trafficking in dangerous drugs;
    (b) Possession of a dangerous drug for the purpose of trafficking
5. Unlawful possession of a firearm or ammunition
6. Offences involving a terrorist act
7. Trafficking in persons or trafficking in children
8. Offences involving child pornography
9. Offences involving fraud
10. Offences involving corruption
11. Offences involving money laundering
12. Offences affecting critical infrastructure
13. Tax offences

Passed in the House of Representatives this day of , 2017.

Clerk of the House

IT IS HEREBY CERTIFIED that this Act is one the Bill for which has been passed by the House of Representatives and at the final vote thereon in the House has been supported by the votes of not less than three-fifths of all the members of the House, that is to say, by the votes of members of the House.

Clerk of the House

I confirm the above.

Speaker

Passed in the Senate this day of , 2017.

Clerk of the Senate

IT IS HEREBY CERTIFIED that this Act is one the Bill for which has been passed by the Senate and at the final vote thereon in the Senate has been supported by the votes of not less than three-fifths of all the members of the Senate, that is to say, by the votes of Senators.

Clerk of the Senate

I confirm the above.

President of the Senate