REPUBLIC OF VANUATU

BILL FOR THE CYBERCRIME ACT NO. OF 2021

Explanatory Note

This Bill provides for the Cybercrime Act.

Cybercrime is a global phenomenon that poses threats to Vanuatu's national infrastructure, public service delivery, commercial and financial security.

The Government in recognising the need to deal with these threats, worked in collaboration with the Council of Europe and the Australian Attorney General's Department to combat cybercrime and to protect the legitimate interests in the use and development of information technologies.

This Bill will achieve the following Policies and Strategies:

(a) Priority 5, Strategy 5.1 – Cybersecurity Policy of the National ICT Policy; and

(b) Goal 3, Objectives 1 and 2 of the Cyber Security Policy; and

(c) Action Plan 1 and Government Direction 1 under Pillar 5 of the National Security Policy; and

(d) Policy objectives 2.4 and 2.9 under Economy Goals of the National Sustainable Development Plan 2016 – 2030.

The main objectives of this Bill are:

(a) to cover the criminalization and sanctioning of unauthorised actions committed by a person in different forms on and through a computer system; and

(b) to cover the criminalization and sanction provisions and other related provisions in the area of computer related crimes. The aim is to protect individuals from offences that are facilitated by and through a computer system; and

(c) to provide for the power and procedure for the obtaining and collecting of electronic evidence; and

(d) to provide privacy safeguards and police accountability when carrying out their duties; and

(e) to provide for an effective and efficient mechanism for international cooperation involving other States in providing a rapid flow of information and evidence.

Prime Minister

REPUBLIC OF VANUATU

BILL FOR THE CYBERCRIME ACT NO. OF 2021

Arrangement of Sections

REPUBLIC OF VANUATU

BILL FOR THE CYBERCRIME ACT NO. OF 2021

An Act to regulate the use of computer systems, programs and data and for related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY

1 Interpretation

In this Act, unless the contrary intention appears:

authorised officer means a police officer appointed as an authorised officer under section 69;

authorised representative means:

(a) the Chief Executive Officer or Managing Director of a service provider or a body corporate of which the service provider is a subsidiary; or

(b) the Secretary of a service provider or a body corporate of which the service provider is a subsidiary; or

(c) an employee authorised, in writing, by the Managing Director or Secretary of a service provider or a body corporate of which the service provider is a subsidiary;

child means a person under the age of 18 years;

Commissioner means the Commissioner of Police appointed under the Police Act [CAP 105];

communication means transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by electronic means;

computer data includes:

(a) data entered or copied into a computer system; and

(b) data held in a removable storage medium in a computer system; and

(c) data held in a computer storage medium on a computer network of which the computer system forms part; and

(d) data held in other computer storage mediums including cloud; and

(e) any representation of information, knowledge, facts, concepts or instruction, which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or a computer network; and

(f) any form, whether readable only by a computer or only by a human or by either, including, but not limited to computer printouts, magnetic storage media, punched cards or stored internally in the memory of the computer;

computer network means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities;

computer storage medium means any article or material from which information is capable of being reproduced, with or without the aid of any other article or device;

computer system means:

(a) a computer; or

(b) two or more interconnected computers; or

(c) any communication links between computers or to remote terminals or another device; or

(d) two or more interconnected computers combined with any communication links between computers or to remote terminals or another device,

which also includes any part of the items described in paragraphs (a) to (d),and all related inputs, outputs, processing, storage, software or communication facilities, the cloud, and stored data;

computer warrant means a warrant granted under section 40;

content data means the substance of a specified communication that is intercepted;

Court means the Supreme Court of Vanuatu;

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

data storage medium means anything that contains or designed to contain data for use by a computer system;

device means any hardware or equipment which performs one or more specific functions and operates on any form or combination of electrical energy and includes but is not limited to:

(a) components of computer systems such as computers, graphic cards, mobile phones or memory chips; or

(b) storage components such as hard drives, memory cards, compact discs or tapes; or

(c) input devices such as keyboards, mouses, track pads, scanners or digital cameras; or

(d) output devices such as printers or screens;

foreign country has the same meaning as in the Mutual Assistance in Criminal Matters Act [CAP 285];

foreign serious offence has the same meaning as in the Proceeds of Crime Act [CAP 284];

information means information, whether in the form of data, text, sounds, images or in any other form;

intelligible output means information from a computer system in whatever form that is able to be read and understood;

interception means the monitoring or recording of non-public transmissions of data to, from or within a computer system;

interception device has the same meaning as in the Police Powers Act No. 37 of 2017;

interception warrant means a warrant granted under section 30;

makes available includes, but not limited to, describing how to obtain access, or describing methods that are likely to facilitate access;

Minister means the Minister responsible for Information Communication and Technology;

Mutual Assistance in Criminal Matters Act means the Mutual Assistance in Criminal Matters Act [CAP 285];

police officer means any member of the Vanuatu Police Force established by the Police Act [CAP 105];

program means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function and make references to a program including references to part of a program;

real time means when information is being generated or transmitted;

serious offence has the same meaning as in the Proceeds of Crime Act [CAP 284];

service provider means:

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

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

(c) a service provider under the Telecommunications, Radiocommunications and Broadcasting Regulation Act No. 30 of 2009;

specified offence means an offence against a law of Vanuatu for which the maximum penalty is imprisonment for a term not exceeding 4 years;

subscriber data:

(a) means any data held by a service provider (whether in the form of computer data or any other form) in relation to a person using or renting its services (a "subscriber") by which the following can be established:

(i) the type of service used, the technical provisions taken in relation to the service and the period of service; and

(ii) 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; and

(iii) any other data on the site of the installation of the equipment needed to use the service, available on the basis of the service agreement or arrangement; and

(b) does not include traffic or content data;

traffic data means electronic data that:

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

(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;

urgent computer warrant means a warrant granted under section 44;

urgent interception warrant means a warrant granted under section 32.

2 Purpose

The purpose of this Act is:

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

(b) to prevent the abusive use of computer systems, programs and data; and

(c) to enable the gathering of forensic material for the investigation and prosecution of breaches of this Act; and

(d) to facilitate international co-operation.

PART 2 COMPUTER OFFENCES

3 Illegal access

(1) For the purposes of this section, **critical infrastructure** means vital computer systems, physical facilities, processes, supply chains, information technologies, communication networks, devices, public utilities and essential services.

(2) A person who intentionally and without lawful excuse, accesses the whole or part of a computer system by infringing a security measure, commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or

(b) in the case of a body corporate-to a fine not exceeding VT4,000,000.

(3) A person who intentionally and without lawful excuse, accesses the whole or part of a critical infrastructure, commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT4,000,000.

(4) A person does not commit an offence under this section if that person:

(a) is entitled to have access to the program or data; or

(b) has consent to have access to the program or data.

4 Illegal interception

(1) A person must not intentionally and without lawful excuse, intercept by any technical means:

(a) any non-public transmission of computer data to, from or within a computer system; or

(b) electromagnetic emission from a computer system carrying such computer data.

(2) Despite subsection (1), the Commissioner may, by Order, authorise for the interception of any non-public transmission or electromagnetic emission.

(3) A person who intentionally and without lawful excuse, intercepts the whole or part of a critical infrastructure, commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT4,000,000.

5 Unauthorised interference

(1) For the purposes of this section, **unauthorised interference** means:

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

(b) the person does not have consent to the interference from a person who is entitled.

(2) A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, commits an offence and is liable on conviction

(a) in the case of an individual- to a fine not exceeding VT7,000,000 or to a term of imprisonment not exceeding 40 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT100,000,000.

(3) A person who causes an unauthorised interference resulting in serious harm in all or any of the following:

(a) a financial loss of more than VT1,000,000;

(b) threatens national security;

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

(d) threatens public health or public safety,

commits an offence and is liable on conviction:

(a) in the case of an individual-to a fine not exceeding VT50,000,000or to a term of imprisonment not exceeding 50 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT100,000,000.

(4) A person who recklessly causes an unauthorised interference commits an offence and is liable on conviction:

(a) in the case of an individual- to, a fine not exceeding VT10,000,000 or to a term of imprisonment not exceeding 40 years, or both;

(b) in the case of a body corporate- to a fine not exceeding VT100,000,000.

(5) For the purposes of this section, it is immaterial that the unauthorised interference is not directed at:

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

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

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

(6) In addition to subsection (5), it is immaterial whether an unauthorised interference or any intended effect of it is permanent or temporary.

6 Misuse of devices

(1) A person who intentionally or without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available:

(a) a software, computer system or an electronic device; or

(b) a password, access code or similar data by which the whole or any part of a computer system or electronic data that is capable of being accessed,

for intercepting or unauthorised interference, commits an offence and is liable on conviction

(i) in the case of an individual- to a fine not exceedingVT1,000,000, or to a term of imprisonment not exceeding 3 years, or both; or

(ii) in the case of a body corporate- to a fine not exceeding VT3,000,000.

(2) Despite subsection (1), it is not an offence under this section if:

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

(b) any undertaking is to comply with a Court order issued or in exercise of any power under this Act or any other Act.

PART 3 COMPUTER RELATED OFFENCES

7 Child pornography

(1) For the purposes of this section, **child pornography** includes any material, but not limited to any audio, visual or text material that represents:

(a) a child engaged in sexually explicit conduct; or

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

(c) images, animations or videos representing a child engaged in sexually explicit conduct.

(2) A person who intentionally or without lawful excuse:

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

(b) offers or solicits, or makes available child pornography through a computer system; or

(c) distributes or transmits child pornography through a computer system; or

(d) obtains or solicits child pornography through a computer system for personal use or for another person; or

(e) possesses child pornography in a computer system or on an electronic storage medium,

commits an offence and is liable on conviction

(a) to a fine not exceedingVT5,000,000 or to a term of imprisonment not exceeding10 years, or both; or

(b) in the case of a body corporate- to a fine not exceedingVT15,000,000.

8 Hosting child pornography

(1) A person commits an offence if the person:

(a) is a service provider; and

(b) is aware, or becomes aware, that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe:

(i) is a child pornography material; and

(ii) does not refer details of the material to the Vanuatu Police Force within a reasonable time after becoming aware of the existence of the material.

(2) A person who commits an offence under subsection (1), is liable on conviction:

(a) in the case of an individual-to a fine not exceeding VT5,000,000 or to a term of imprisonment not exceeding 10 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT10,000,000.

9 Identity- related crime

A person who intentionally or without lawful excuse uses a computer system:

(a) to transfer; or

(b) to possess; or

(c) to use,

the identification of another person with the intention to commit, aid or abet or connect with any unlawful activity, commits an offence and is liable on conviction:

(i) in the case of an individual- to a fine not exceedingVT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(ii) in the case of a body corporate- to a fine not exceeding VT5,000,000.

10 Cyber stalking

(1) For the purposes of this section, **cyber stalking** means an act to coerce, intimidate, harass, insult or annoy a person through computer systems or electronic devices.

(2) A person who, directly or indirectly, uses any electronic communication for cyber stalking, commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT1,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT3,000,000.

11 Solicitation of children

An individual who uses a computer system:

(a) to propose to a child or

(b) to propose to someone that the person believes to be a child,

to meet him or her or another person with the intention that the child be sexually exploited by him or her or another person, whether or not such proposal has been followed by material acts, commits an offence and is liable on conviction to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both.

12 Computer related forgery

A person who intentionally and without lawful excuse, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable or intelligible and wrongfully:

(a) gains; or

(b) inputs; or

(c) alters; or

(d) deletes; or

(e) suppresses,

electronic data, commits an offence and is liable on conviction:

(i) in the case of an individual- to a fine not exceedingVT5,000,000, or to a term of imprisonment not exceeding 12 years, or both; or

(ii) in the case of a body corporate- to a fine not exceedingVT10,000,000.

13 Computer related fraud

A person who intentionally and without lawful excuse causes a loss of property to another person by:

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

(b) any interference with the functioning of a computer system,

with fraudulent intent of procuring personal gain for another person, commits an offence and is liable on conviction:

(i) in the case of an individual- to a fine not exceedingVT5,000,000, or to a term of imprisonment not exceeding 12 years, or both; or

(ii) in the case of a body corporate- to a fine not exceeding VT10,000,000.

14 Illegal access with intent to commit or facilitate further offences

(1) A person is guilty of an offence under this section if the person commits an offence, under section 3, with the intent:

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by the person committing the offence or by any other person),

and the offence the person intends to commit or facilitate is a further offence.

(2) It is immaterial for the purposes of this section whether the further offence is committed on the same occasion as the unauthorised access offence or on any future occasion.

(3) A person may be charged with an offence under this section even though the facts are such that the commission of the further offence is impossible.

(4) A person who intentionally accesses, without lawful excuse, the whole or any part of a computer system and commits or facilitates a further offence, is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT7,000,000 or to a term of imprisonment not exceeding 7 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT9,000,000.

PART 4 PROCEDURES

Division 1 Disclosure of information, assistance and production of computer data

15 Disclosure of information of an investigation

(1) For the purposes of this section, a **service provider** includes all or any employee, agent and contractor of the service provider.

(2) A service provider who receives an order from a Court, relating to a criminal investigation that provides that confidentiality is to be maintained or such obligation is stated by law and the service provider discloses or continues to disclose:

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

(b) anything done under the order; or

(c) any data collected or recorded under the order,

commits an offence and is liable on conviction:

(i) in the case of an individual-to a fine not exceeding VT2,000,000, or to a term of imprisonment not exceeding 5 years, or both; or

(ii) in the case of a body corporate- to a fine not exceeding VT5,000,000.

16 Assistance

A person who is not a suspect of a crime under this Act, but is in possession or control of a device or data that is subject to a computer warrant under Division 6, must, at his or her own cost, permit or assist an authorised officer when carrying out the search:

(a) to access and use the device or data; and

(b) to obtain a copy of that data; and

(c) to use the device to make copies; and

(d) to obtain an intelligible output from a device in a format that can be read.

17 Production of computer data

(1) This section applies if a police officer makes an application to the Court that data held in a data storage medium, or a computer network or a computer system, or a printout or any other information, is reasonably necessary for a criminal investigation or a proceeding that involves a specified offence against the laws of Vanuatu or a serious offence against the laws of a foreign country.

(2) The Court may order:

(a) a person in control of the data storage medium, the computer network or the computer system to produce in a manner specified in the order a specified data or a printout or other intelligible output of that data; and

(b) a person who has access to a specified computer system process to compile the data held in the system and give it to a specified person.

(3) Prior to making an order under subsection (2), the Court must consider the following:

(a) the seriousness of the offence to which the criminal investigation or proceeding relates; and

(b) the reliability of the information on which the application is based, including the nature of the source of the information; and

(c) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and

(d) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

(e) whether any condition should be included in the order; and

(f) any other matter that the Court considers relevant.

Division 2 Preservation Order

18 Preservation order

(1) The Commissioner may, for the purposes of retaining computer data, including traffic data or content data, in a person's possession or control, apply to Court for a preservation order.

(2) The Court may grant a preservation order if it is satisfied on reasonable grounds that the preservation of the computer data is reasonably necessary for law enforcement purposes or for a criminal investigation or proceeding involving a serious offence against a law of a foreign country.

(3) A preservation order:

(a) comes into force when the service provider receives it; and

(b) remains in force for the period stated in the preservation order or until revoked by the Court under section 19.

(4) A preservation order must not remain in force for a period exceeding 90 days.

(5) Despite subsection (4), if the Court is satisfied that more time is needed to obtain what is required under the preservation order, the Court may extend the period for which the preservation order is in force, for another 90 days.

(6) A person issued with a preservation order must keep the order and all information in the order confidential.

(7) A person who, without reasonable excuse fails:

(a) to comply with an order granted under subsection (2);or

(b) to keep all information about the order confidential as provided under subsection (6),

commits an offence and is punishable on conviction:

(i) in the case of an individual-to a fine not exceeding VT1,000,000, or to a term of imprisonment not exceeding 3 years, or both; or

(ii) in the case of a body corporate-to a fine not exceeding VT2,000,000.

19 Revocation of preservation order

(1) If the Court is satisfied on reasonable grounds that the preservation order is no longer required, it is to revoke the preservation order any time before it expires.

(2) If a preservation order is revoked, a police officer must immediately notify the service provider or its authorised representative about the revocation, and provide the service provider or its authorised representative a copy of the revocation.

20 Service provider or authorised representative to disclose traffic data

A service provider or its authorised representative issued with a preservation order must disclose, as soon as practicable, sufficient amount of traffic data to enable a police officer to identify any other service providers involved in the transmission of the communication.

Division 3 Subscriber data, traffic data and content data

21 Request for disclosure of subscriber data

(1) The Commissioner may, in writing, request a service provider to disclose subscriber data if he or she is satisfied that the disclosure is necessary:

(a) for law enforcement purposes; or

(b) for the enforcement of a foreign serious offence under the Mutual Assistance in Criminal Matters Act.

(2) A service provider must comply with the request under subsection (1), as soon as practicable, after receiving the request.

(3) A service provider who fails to comply with subsection (2), commits an offence and is liable on conviction to a fine not exceeding VT1,000,000.

22 Request for disclosure of traffic data

(1) The Commissioner may, in writing, request a service provider to disclose records of traffic data that came into existence before the time the disclosure is sought, if the disclosure is reasonably necessary:

(a) for law enforcement purposes; or

(b) for the enforcement of a foreign serious offence made under the Mutual Assistance in Criminal Matters Act.

(2) Prior to making a request under subsection (1), the Commissionerm ust:

(a) be satisfied that the public interest in the disclosure of the data substantially outweighs the right to privacy of a person whose privacy may be affected as a result of the disclosure; and

(b) consider any matters relevant to giving the approval, including the following:

(i) the volume and nature of the data to be disclosed; or

(ii) the gravity of the conduct being investigated; or

(iii) the likely usefulness of the data to the investigation; or

(iv) the purpose for which access to the data is requested.

(3) A service provider must comply with a request under subsection (1), as soon as practicable, after receiving the request.

(4) A service provider who fails to comply with subsection (3) commits an offence and is liable on conviction to a fine not exceeding VT2,000,000.

23 Request for access to traffic data in real time

(1) The Commissioner may, in writing, request a service provider to provide access to records of traffic data in real time for up to 90 days, if the access is reasonably necessary for:

(a) the enforcement of an offence punishable, on conviction, by imprisonment for a term not exceeding 2 years under this Act or any other Act; or

(b) for the enforcement of a foreign serious offence made under the Mutual Assistance in Criminal Matters Act.

(2) Prior to making a request under subsection (1), the Commissioner must:

(a) be satisfied that the public interest in accessing the records substantially outweighs the right to privacy of a person whose privacy may be affected as a result of the access; and

(b) consider any matters relevant to giving the approval, including the following:

(i) the volume and nature of the records to be disclosed; or

(ii) the gravity of the conduct being investigated; or

(iii) the likely usefulness of the records to the investigation; or

(iv) the purpose for which access to the records is requested.

(3) The Commissioner must, in writing, cancel a request under subsection (1) any time before it expires, if he or she is satisfied that the request is no longer required.

(4) The Commissioner must, in writing, notify the service provider or an authorised representative about the cancellation under subsection (3), and provide a copy of the cancellation immediately after the request is cancelled.

24 Disclosure of content data

(1) An authorised officer may apply to the Court for an order to allow access to and disclosure of content data as follow:

(a) a person engaged in, or suspected on reasonable grounds to be engaged in, the commission of:

(i) a specific offence; or

(ii) a foreign serious offence under the Mutual Assistance in Criminal Matters Act, and

(b) a service that has been used, is being used or is likely to be used by a person under paragraph (a).

(2) The authorised officer in making an application under subsection (1), is to state in the application:

(a) the details of each service provider subject to the order; and

(b) the offence or offences to which the application relates; and

(c) the information and evidence relied upon; and

(d) if a preservation order has been issued.

(3) The authorised officer is to provide to the Court any further information as the Court may require concerning the grounds on which the order is sought.

25 Subscriber data, traffic data and content data to be used for lawful purposes only

(1) Subscriber data obtained under section 21 is to be used:

(a) for the purposes for which it was originally obtained; or

(b) to enforce any criminal law imposing a pecuniary penalty, or to protect the public revenue; or

(c) to enforce a foreign forfeiture order or a foreign pecuniary penalty order in connection with a foreign serious offence under the Mutual Assistance in Criminal Matters Act.

(2) Traffic data obtained in real time is to be used:

(a) for the purpose for which it was originally obtained; or

(b) to enforce any criminal law imposing a pecuniary penalty, or to protect the public revenue; or

(c) to enforce a foreign serious offence according to an authorisation made under the Mutual Assistance in Criminal Matters Act.

(3) Content data preserved under section 18is to be used:

(a) for the purposes for which the content data was originally obtained; or

(b) to enforce a specified offence or an offence under this Part; or

(c) to enforce a foreign serious offence according to an authorisation made under the Mutual Assistance in Criminal Matters Act.

(4) If the Commissioner is satisfied that the information obtained is no longer required, the Commissioner must arrange for the destruction of the data and any reproduction of the data to be under the control of the Vanuatu Police Force.

Division 4 Disclosure to a foreign law enforcement agency

26 Disclosure to a foreign law enforcement agency

(1) Information obtained under this Part must not be disclosed to a foreign law enforcement agency unless the disclosure has been authorised by the Commissioner.

(2) The Commissioner must not authorise a disclosure under this Part, unless he or she is satisfied that:

(a) the disclosure is reasonably necessary for the enforcement of a foreign serious offence; and

(b) is appropriate in all the circumstances.

Division 5 Interception warrant

27 Commissioner to authorise applications

(1) The Commissioner may authorise an application for:

(a) an interception warrant; or

(b) the renewal of an interception warrant; or

(c) an urgent interception warrant.

(2) The Commissioner must not authorise an application referred to in subsection (1), unless the Commissioner is satisfied that there are reasonable grounds to suspect that a person:

(a) is planning, participating in or committing a specified offence; or

(b) has planned, participated in or committed a specified offence.

28 Application for interception warrant

(1) If the Commissioner has authorised an application for an interception warrant under section 27, a police officer is to apply to the Court to grant the interception warrant to:

(a) intercept a private communication by means of an interception device; or

(b) record visually or observe an activity of a person by means of an interception device; or

(c) use both an interception device and an optical surveillance device.

(2) The application must be in writing and made on oath by a police officer, and must set out:

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

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

(c) the facts relied upon to demonstrate that there are reasonable grounds for suspecting that a person is planning, participating in or committing, or has planned, participated in or committed, a specified offence; and

(d) a description of the manner in which it is proposed to intercept private communications or record or observe activities; and

(e) the extent to which other methods for the investigation of the offence, other than an interception warrant, have been used by or are available to the police officer; and

(f) either:

(i) the name and address, if known, of the person whose private communications or a record or observations of whose activities there are reasonable grounds for suspecting will assist the police investigation of the case; or

(ii) if the name and address of the suspect are not known, a general description of the premises, place, item or type of facility in respect of which it is proposed to intercept private communications or record or observe activities; and

(g) the period for which a warrant is requested.

(3) For the purpose of this section, **optical surveillance device** has the same meaning as in the Police Powers Act No. 37 of 2017.

29 Content and terms of an interception warrant

(1) An interception warrant must be in the prescribed form and state the following information:

(a) the offence or offences in respect of which the warrant is granted; and

(b) if the warrant relates to the use of an interception device on premises:

(i) the name and address of the suspect whose private communications may be intercepted or whose activities may be recorded or observed; or

(ii) if the suspect's name and address are not known, a general description of the premises, place, item or type of facility in respect of which the private communications will be intercepted or activities recorded or observed; and

(c) if the warrant authorises the use of an interception device in respect of the conversations, activities or location of a person, state the name of the person (if known) or the fact that the person's identity is unknown; and

(d) any other terms and conditions that the Court considers necessary for the purpose of public interest.

(2) An interception warrant has the effect, according to its terms, of authorising:

(a) the interception of private communications by means of an interception device; or

(b) the recording visually or observing of an activity of a person by means of an interception device; or

(c) activities referred to in paragraphs (a) and (b).

(3) In addition to subsection (2), an interception warrant authorises:

(a) the retrieval of an interception device; and

(b) the entry, with such reasonable force as necessary, to any premises for the purposes of placing, servicing or retrieving an interception device; and

(c) the connection of the interception device to any source of electricity and the use of electricity from that source to operate the device; and

(d) the provision of assistance or technical expertise to the police officer primarily responsible for the execution of the warrant in the installation, use, maintenance or retrieval of the interception device.

(4) If the warrant authorises the placing of an interception device in a residential or business premises of:

(a) a lawyer, clergyman or a medical practitioner; or

(b) a person specified by the Court,

the Court may attach conditions that it considers necessary to avoid, as far as practicable, the interception of information or recording or observing of activities of a professional character to which the lawyer, clergyman, medical practitioner or such other person specified by the Court is a party.

(5) To avoid doubt, an interception warrant is not limited to a particular premises, and can apply in relation to an interception device designed to intercept communications, or observe or record activities involving a person wherever that person may be.

30 Granting of an interception warrant

(1) The Court may grant an interception warrant if it is satisfied that there are reasonable grounds:

(a) to suspect that a person is planning, participating in or committing, or has planned, participated in or committed, a specified offence; and

(b) to believe that evidence relevant to the investigation of a case will be obtained through the use of an interception warrant to intercept private communications, records or observe activities; and

(c) the proposed interception is justified by the social harm of the suspected offence against which it is directed.

(2) In addition to subsection (1), the Court, prior to granting an interception warrant, must consider the following:

(a) the seriousness of the offence to which the criminal investigation or proceeding relates; and

(b) the reliability of the information on which the application is based, including the nature of the source of the information; and

(c) if the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person, whose privacy may be affected as a result of the production; and

(d) if there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

(e) if any condition should be included in the warrant; and

(f) if the foreign country has made a request for mutual assistance under this Act or the Mutual Assistance in Criminal Matters Act and the Public Prosecutor has authorised the use of a lawful investigative power; and

(g) any other matters that the Court considers relevant.

31 Period and extension of interception warrant

(1) An interception warrant is valid for the period specified in the warrant, being a period not exceeding 90 days.

(2) Subject to subsection (1), the Court may grant an extension of an interception warrant upon an application made before the warrant expires.

(3) An application for an extension of an interception warrant must:

(a) provide the reason and period for which the renewal is required; and

(b) be accompanied by full particulars, together with times and dates, of any interceptions made or attempted under the interception warrant and an indication of the nature of the information that has been obtained by such interception; and

(c) be supported by such other information as the Court may consider necessary.

(4) The Court may extend an interception warrant if it is satisfied that the circumstances described in section 30 still apply.

32 Urgent interception warrant

(1) The Court may grant an urgent interception warrant if it is satisfied that:

(a) the circumstances to which the application relates are urgent; or

(b) the delay that would be caused by the application being made in person would frustrate the effective execution of the warrant.

(2) A police officer may make an application for an urgent interception warrant orally, by telephone, email, facsimile or other electronic means.

(3) The Court may, orally or in writing, grant an urgent interception warrant:

(a) for the interception of private communications; or

(b) for the recording of activities in respect of a particular premises; or

(c) for a particular person; or

(d) for a particular place; or

(e) for a particular item; or

(f) for a particular type of facility,

and in a particular manner.

(4) The contents and terms of an interception warrant under section 29 apply to the contents and terms of an urgent interception warrant.

(5) An urgent interception warrant is valid for 48 hours commencing from the time on which it is issued.

(6) Subject to subsection (1), the Court must, as soon as practicable, give a copy of the warrant to a police officer who applied for the urgent interception warrant under subsection (2).

(7) If it is not reasonably practicable for the Court to give a copy of the urgent interception warrant to the police officer:

(a) the Court must inform the police officer of the terms of the urgent interception warrant and the date and time the warrant was signed; and

(b) the police officer must make a record of the following details:

(i) the name of the Judge who issued the urgent interception warrant; and

(ii) the date and time the urgent interception warrant was signed.

33 Service provider to be served with interception warrant

(1) If an interception warrant is issued under this Division to intercept a private communication, the authorised officer must:

(a) inform the service provider about the warrant; and

(b) serve a copy of the warrant to the service provider.

(2) The service provider must comply with the warrant as soon as it is served.

34 Admissibility of evidence

(1) Any information or recording obtained pursuant to an interception warrant or an urgent interception warrant is admissible as evidence in any proceedings for the prosecution of a specified offence.

(2) Any information or recording obtained in breach of subsection 29(4) is not admissible evidence.

35 Minor defect in connection with interception warrant or urgent interception warrant

(1) This section applies if:

(a) information or a recording is purportedly obtained through the use of an interception device authorised under an interception warrant or an urgent interception warrant; and

(b) there is a minor defect or irregularity in relation to the interception warrant or urgent interception warrant and, but for that defect or irregularity, the interception warrant or urgent interception warrant would have been sufficient authority for the action taken.

(2) This section applies if:

(a) the use of the interception device is to be taken as being valid; and

(b) any information or recording obtained pursuant to the interception warrant or urgent interception warrant is admissible as evidence as if the interception warrant or urgent interception warrant did not have that defect or irregularity.

(3) A reference in subsection (1), to a defect or irregularity in relation to an interception warrant or urgent interception warrant is a reference to a defect or irregularity (other than a substantial defect or irregularity):

(a) in, or in connection with, the issue of, a document purporting to be that interception warrant or urgent interception warrant; or

(b) in connection with the execution of that interception warrant or urgent interception warrant or the execution of a document purporting to be that interception warrant or urgent interception warrant.

36 Prohibition on disclosure of communications intercepted and recordings

(1) A person who:

(a) intercepts or assists in the interception of a private communication in accordance with an interception warrant or urgent interception warrant; or

(b) acquires knowledge of a private communication as a direct or indirect result of that interception; or

(c) makes a record of the activities of a person,

is prohibited to disclose in whole or in part the substance or meaning of that communication or recording.

(2) A person who contravenes subsection (1) commits an offence punishable on conviction:

(a) in the case of an individual- to a fine not exceeding VT2,000,000 or a term of imprisonment not exceeding 5 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT4,000,000.

37 Revocation of interception warrant or an urgent interception warrant

(1) A police officer may, at any time, apply to the Court to revoke an interception warrant or an urgent interception warrant.

(2) The Court must revoke an interception warrant or an urgent interception warrant if it is satisfied that the warrant is no longer required.

(3) If an interception warrant or urgent interception warrant to intercept a private communication is revoked, the police officer must notify the service provider's or its authorised representative about the revocation, and give the service provider or its authorised representative a copy of the revocation, immediately after the warrant is revoked.

Division 6 Provisions relating to computer warrants

38 Commissioner to authorise applications

(1) The Commissioner may authorise an application for:

(a) a computer warrant or renewal of a computer warrant; or

(b) an urgent computer warrant.

(2) The Commissioner must not authorise an application referred to in subsection (1), unless the Commissioner is satisfied that there are reasonable grounds to suspect that there may be on the person or at the place a data storage medium, or a computer network or a computer system that:

(a) may be material evidence of the commission of a specified offence; or

(b) may be material evidence of the commission of a foreign serious offence; or

(c) has been acquired by a person as a result of the commission of an offence.

39 Application for a computer warrant

(1) If the Commissioner has authorised an application for a computer warrant under section 38, an authorised officer is to apply to the Court to grant a computer warrant to access:

(a) a place specified in the warrant; or

(b) a data storage medium at the location specified in the warrant; or

(c) a computer network at the location specified in the warrant; or

(d) a computer system at the location specified in the warrant.

(2) An application must be in writing and made on oath by an authorised officer, and must set out:

(a) if a person is to be searched, the person's name, age and address; and

(b) if a place is to be searched:

(i) a description of the place to be searched; and

(ii) if the place is occupied, the name and age of any occupiers of the place, if known; and

(c) the offence to which the application relates; and

(d) a description of the nature of the data storage medium, computer network, computer system or suspected to be evidential material; and

(e) the information relied on to support the reasonable suspicion that evidence on the commission of an offence:

(i) is in or under the control of the person or at the place when the computer warrant is executed; or

(ii) is likely to be in or under the control of the person or at the place when the computer warrant is executed; and

(f) if a computer warrant was issued previously in relation to the person or place; and

(g) if authority to execute the computer warrant at night is being sought, why it is necessary to execute the computer warrant at night; and

(h) the period the computer warrant is required.

40 Granting of computer warrant

(1) The Court may grant a computer warrant if the Court is satisfied with the application of the authorised officer made under section 39.

(2) Without limiting subsection (1), prior to granting a computer warrant, the Court must consider the following:

(a) the seriousness of the offence to which the criminal investigation or proceeding relates; and

(b) the reliability of the information on which the application is based, including the nature of the source of the information; and

(c) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and

(d) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

(e) whether any condition should be included in the computer warrant; and

(f) the proposed duration of the computer warrant; and

(g) any other matters that the Court considers relevant.

41 Contents of computer warrant

A computer warrant must state the following information:

(a) if a person is to be searched, the person's name, age and address; and

(b) if a place is to be searched:

(i) a description of the place to be searched; and

(ii) if the place is occupied, the name and age of any occupiers of the place, if known; and

(c) the offence to which the application relates; and

(d) the types of evidential material that may be searched for; and

(e) the power of the authorised officer to secure or render inaccessible a data storage medium, computer network or computer system; and

(f) the date and time the computer warrant expires; and

(g) any conditions imposed in relation to executing the computer warrant.

42 Extension of a computer warrant

(1) The Court must specify in the computer warrant the date and time the computer warrant expires.

(2) The Court may extend the date and time, when a computer warrant expires, if it is satisfied that the purpose for which the warrant was granted cannot be satisfied before the warrant is expired.

43 Application for an urgent computer warrant

(1) If the Commissioner has authorised an application for an urgent computer warrant under section 38, an authorised officer may apply to the Court to grant an urgent computer warrant to access:

(a) a place specified in the warrant; or

(b) a data storage medium at the location specified in the warrant; or

(c) a computer network at the location specified in the warrant; or

(d) a computer system at the location specified in the warrant.

(2) An authorised officer may make an application for an urgent interception warrant orally, by telephone, email, facsimile or other electronic means.

(3) The authorised officer in making an application under subsection (2) must set out:

(a) if a person is to be searched, the person's name, age and address; and

(b) if a place is to be searched:

(i) a description of the place to be searched; and

(ii) if the place is occupied, the name and age of any occupiers of the place, if known; and

(c) the offence to which the application relates; and

(d) a description of the nature of the data storage medium, computer network, computer system or suspected to be evidential material; and

(e) the information relied on to support the reasonable suspicion that evidence on the commission of an offence:

(i) is in or under the control of the person or at the place; or

(ii) is likely to be in or under the control of the person or at the place when an urgent computer warrant is executed; and

(f) if an urgent computer warrant was issued previously in relation to the person or place; and

(g) if authority to execute an urgent computer warrant at night is being sought, why it is necessary to execute the urgent computer warrant at night; and

(h) the period an urgent computer warrant is required.

(4) The authorised officer must a soon as practicable, after the granting of the urgent computer warrant, send his or her application, in writing, to the Court.

44 Granting of an urgent computer warrant

(1) The Court may grant an urgent computer warrant if the Court is satisfied with the application of the authorised officer made under section 43.

(2) Without limiting subsection (1), prior to granting an urgent computer warrant, the Court must consider the following:

(a) the urgency of the situation requiring an urgent computer warrant; and

(b) the seriousness of the offence to which the criminal investigation or proceeding relates; and

(c) the reliability of the information on which the application is based, including the nature of the source of the information; and

(d) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and

(e) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

(f) whether any condition should be included in the urgent computer warrant; and

(g) the proposed duration of the urgent computer warrant; and

(h) any other matters that the Court considers relevant.

45 Effects of a computer warrant and an urgent computer warrant

(1) An authorised officer is authorised, under a computer warrant or an urgent computer warrant granted under sections 40 and 44,to:

(a) seize an item that the authorised officer believes on reasonable grounds to be:

(i) evidential material in relation to an offence to which the warrant relates; or

(ii) evidential material that is relevant to another offence under this Act or any other Act; and

(b) access a data storage medium, or a computer network or a computer system for the purposes of obtaining information and records, and collate, copy or extract data; and

(c) access, seize or secure any equipment, data storage medium, or other item by which information, records or data may be stored; and

(d) require a person with a knowledge of a data storage medium, or a computer network or a computer system to assist the authorised officer in accessing the data storage medium, the computer network or the computer system; and

(e) if an authorised officer suspects on reasonable grounds that the data that is accessible from the computer system might be the data

that could be accessed, collated or seized under the warrant, or other item under paragraph(a), the authorised officer may:

(i) operate the computer system to access the data; or

(ii) operate another computer system accessible from the computer system operated under subparagraph (i) to access data; or

(iii) copy any or all of the data to another data storage medium or a computer network or a computer system; or

(iv) if, by using facilities at the place, the data can be put in a documentary form, operate the facilities to put that data in that form and seize the produced documents; and

(f) move data storage medium or a computer network or a computer system at the place searched to another place for examination in order to determine whether it contains data that could be accessed, collated or seized under the warrant if:

(i) the occupier of the place consents; or

(ii) it is significantly more practicable to do so, having regard to the time it will take to copy the data, and there are reasonable grounds to suspect that the data that could be accessed, collated or seized under the warrant; and

(g) do anything reasonably necessary to prevent loss, destruction or damage to anything connected with the offence or any other offence; and

(h) use other authorised officers or persons as reasonably necessary for the execution of the warrant; and

(i) search a person who is at the place when the warrant is executed if the authorise officer suspects, on reasonable grounds, that the person has any evidential material in the his or her possession.

(2) If an authorised officer seizes a data storage medium, a computer network, a computer system, equipment, device or other items under subsection (1), the authorised officer:

(a) may take possession of it; and

(b) may retain it for such a time as he or she considers necessary for the purposes of this Act.

(3) An authorised officer must return any item detained under subsection (2) to its owner if:

(a) it is no longer necessary to seize the item; or

(b) it is decided that the item is not to be used in evidence, except where the authorised officer believes, on reasonable grounds, that the possession of data may constitute an offence.

46 Access to seized data

(1) Subject to subsection (2), on request, a police officer executing a computer warrant may:

(a) allow a person who had the custody or control of the data storage medium, computer network or computer system, or someone acting on the person's behalf, to access and copy of the data; or

(b) give that person a copy of that data held in the computer system.

(2) The police officer may refuse to give access to, or provide copies of data held in a data storage medium, computer network or computer system, if the police officer believes on reasonable grounds that giving the access or providing the copies may:

(a) constitute an offence under this Act or any other Act; or

(b) prejudice a criminal investigation or proceedings.

47 Securing or rendering inaccessible data under a computer warrant or an urgent computer warrant

(1) For the purposes of this section, **expert** means a person qualified in digital forensics.

(2) An authorised officer executing a computer warrant or an urgent computer warrant may do whatever is necessary to secure or render inaccessible a data storage medium, computer network or computer system if the police officer suspects, on reasonable grounds, that:

(a) evidence of the commission of an offence may be accessible by operating the data storage medium, computer network or computer system; and

(b) expert assistance is needed to operate the data storage medium, computer network or computer system; and

(c) if the police officer does not take action under this subsection, the evidence may be destroyed, altered or otherwise interfered with.

(3) The police officer is to, by way of notice, notify the person who has custody or control of the data storage medium, computer network or computer system:

(a) the intention of the police officer to secure or render inaccessible the data storage medium, computer network and computer system; and

(b) that the data storage medium, computer network and computer system may be secured or inaccessible for up to 28 days.

(4) The data storage medium, computer network or computer system may be secured or inaccessible until any of the following occurs:

(a) 28 days after the data storage medium, computer network or computer system is first secured or rendered inaccessible; or

(b) the data storage medium, computer network or computer system has been operated by an expert.

(5) The police officer may apply to the Court for an extension of the time referred in paragraph (4)(a), if, the police officer believes, on reasonable grounds, that the expert assistance will not be available within that time.

(6) The police officer may make more than 1 application under subsection (5) until the expert assistance is available.

(7) The police officer must, by way of notice, notify the person who has custody or control of the data storage medium, computer network or computer system:

(a) the intention of the police officer to apply for an extension; and

(b) that the person is entitled to be heard in relation to the application.

48 Assisting police officer in executing computer warrant

(1) A police officer may direct a person in possession or control of, or with knowledge of, the data storage medium, computer network or computer system to assist the police officer to:

(a) access and operate the data storage medium, computer network or computer system to access any computer data (including data stored at any place or on a separate data storage medium); and

(b) obtain and copy the data; and

(c) use equipment to make copies of the data; and

(d) obtain an intelligible output from the computer system in a format that can be read; and

(e) do anything that the police officer reasonably requires.

(2) A person who fails without reasonable excuse to comply with a direction under subsection (1), commits an offence and is liable on conviction:

(a) in the case of an individual – to a fine not exceeding VT 1,000,000 or a term of imprisonment not exceeding 3 years or both; or

(b) in the case of a body corporate – to a fine not exceeding VT 2,000,000.

49 Exercising reasonable care

(1) For the purposes of this section, **damage,** in relation to data, includes damage by erasing of the data or addition of other data but does not include the reasonable alteration of data by digital forensic processes.

(2) A police officer, or a person assisting the police officer, when examining or retaining a data storage medium, computer network or computer system under a computer warrant or an urgent computer warrant must take reasonable care to prevent any damage to the following:

(a) the data storage medium, computer network or computer system; and

(b) data stored on, or accessed by operating the data storage medium, computer network or computer system; and

(c) programs associated with the use of the data storage medium, computer network or computer system, or with the use of the data stored in the data storage medium, computer network or computer system.

50 Receipt for items seized under computer warrant

(1) For the purpose of this section, **receipt** means an inventory of all items collected during the execution of the computer warrant or urgent computer warrant.

(2) If a computer warrant authorises a police officer to seize an item, the police officer must, after seizing the item, give the person searched or occupier of the place searched, a receipt for the item seized or leave a receipt for the item seized in a noticeable place at the place searched.

(3) The receipt must include sufficient information to identify the following:

(a) the item that was seized; and

(b) the time the item was seized; and

(c) the person who seized the item; and

(d) the place the item was taken; and

(e) the time the item is to be returned.

(4) This section does not apply if a police officer believes, on reasonable grounds, that:

(a) no person appears to be in possession of the item; or

(b) the item is abandoned.

51 Measures to control retention of seized data storage medium, computer network or computer system

(1) A police officer who seizes a data storage medium, computer network or a computer system under a computer warrant or an urgent computer warrant, must, take reasonable steps to reduce the need for extended retention of data storage medium, computer network or computer system as evidence by doing any of the following as soon as practicable:

(a) arranging for the data storage medium, computer network or computer system, or part thereof, to be copied; or

(b) arranging for any necessary test or examination of the data storage medium, computer network or computer system; or

(c) gathering any other available secondary evidence in relation to the data storage medium, computer network or computer system.

(2) Despite subsection (1), a police officer may retain the data storage medium, computer network or computer system for a reasonable time if the police officer believes, on reasonable grounds, that it is necessary to do so to prevent the commission of an offence.

52 Destruction of certain data seized under a computer warrant or an urgent computer warrant

If the Commissioner is satisfied that data accessed or copied under a computer warrant or an urgent computer warrant is no longer useful for law enforcement purposes, the Commissioner must arrange for the destruction of the data, and any reproduction, under the control of the Vanuatu Police Force.

53 Prohibition on disclosure of information, records and data

(1) A person who obtains information, extracts, records or data pursuant to a request, order or warrant under this Part must not knowingly disclose in whole or in part the information, extracts, records or data otherwise in the performance of his or her duties.

(2) A person who contravenes subsection (1), commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT1,000,000, or a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT2,000,000.

54 Evidentiary certificates for service providers

(1) An authorised representative may issue an evidentiary certificate sworn by the authorised representative, setting out the facts, that the authorised representative considers relevant in relation to acts or things done by, or in relation to, the service provider in order:

(a) to comply with a request for disclosure of subscriber data, traffic data or content data under sections 21, 22, and 24; or

(b) to comply with a request for access to traffic data in real time under section 23; or

(c) to comply with a preservation order under Division 2; or

(d) to enable an interception warrant to be executed.

(2) An evidentiary certificate issued under subsection (1):

(a) must be received as evidence in the proceeding without further proof; and

(b) is conclusive evidence of the matters stated in it.

55 Hindering or obstructing the lawful exercise of powers

(1) A person commits an offence if without reasonable excuse that person:

(a) hinders or obstructs a police officer, or a person assisting a police officer, in carrying out his or her duties under this Act; or

(b) intends to hinder or obstruct the police officer or a person assisting the police officer.

(2) A person who commits an offence under subsection (1), is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT1,000,000, or a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT2,000,000.

56 Obligations of service providers

(1) A service provider must prevent communications networks and facilities from being used in, or in relation to, the commission of offences against this Act or any other Act.

(2) A service provider or an authorised representative who receives a request for information under this Act must maintain the confidentiality of any procedures and information relating to the request.

(3) A service provider or an authorised representative, who fails, without reasonable excuse, to comply with subsection (2) commits an offence and is liable on conviction, to a fine not exceeding VT2,000,000.

(4) A service provider or an authorised representative, commits an offence if the service provider or the authorised representative fails to comply with a

lawful request made by a police officer under this Act and is liable on conviction to a fine not exceeding VT2,000,000.

(5) A reference in this section to giving assistance includes a reference to giving such assistance as is reasonably necessary for the following purposes:

(a) enforcing the criminal law and laws imposing pecuniary penalties; and

(b) assisting the enforcement of the criminal laws in force in a foreign country; and

(c) protecting the public revenue; and

(d) safe-guarding national security.

PART 5 INTERNATIONAL COOPERATION

57 General principles relating to mutual assistance

Vanuatu may cooperate with any foreign country, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence pursuant to this Act and the Mutual Assistance in Criminal Matters Act.

58 Public Prosecutor to make and act on mutual assistance requests

(1) The Public Prosecutor may make requests for mutual assistance in any investigation or proceeding commenced in Vanuatu, relating to any computer or computer related offence.

(2) The Public Prosecutor may, in respect of any request from a foreign country for mutual assistance in any investigation or proceeding commenced in that foreign country:

(a) grant the request, in whole or in part, on such terms and conditions as he or she thinks fit; or

(b) refuse according to the terms set out under sections 8, 9 and 10 of the Mutual Assistance in Criminal Matters Act; or

(c) after consulting with the appropriate authority of the foreign country, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Vanuatu.

(3) A mutual assistance request under this section is to be executed according to the procedures specified by the foreign country, except where incompatible with the laws of Vanuatu.

(4) Prior to refusing or postponing assistance, the Public Prosecutor is to, where appropriate after having consulted with the foreign country, consider whether the request may be granted partially or subject to conditions.

(5) The Public Prosecutor is to immediately inform the foreign country of the outcome of the execution of a request for mutual assistance.

(6) In addition to subsection (5), the Public Prosecutor is to inform the foreign country of any reasons:

(a) to render impossible the execution of the request; or

(b) to delay the execution of the request significantly; or

(c) to postpone the request; or

(d) to refuse the request.

(7) The foreign country may request the Public Prosecutor to keep confidential the fact of any request made under this Act or the Mutual Assistance in Criminal Matters Act, as well as its subject, except to the extent necessary for its execution.

(8) If the Public Prosecutor cannot comply with the request for confidentiality under subsection (7), he or she must immediately inform the foreign country, whether the request should still be executed.

(9) Subsections (8) applies *mutatis mutandis* when the Public Prosecutor is the requesting country.

(10) If the foreign country cannot comply with such conditions under subsection (2), it must notify the Public Prosecutor, who will then determine whether the information should still be provided.

(11) If the foreign country accepts the information subject to the conditions, it is to be bound by them.

(12) Subsections (1), (2) and (3) apply *mutatis mutandis* when spontaneous information is provided to the Public Prosecutor by a foreign country.

59 Additional information

(1) The Public Prosecutor may, subject to this Act and without prior request, forward to a foreign country information obtained within the framework of his or her own investigations when he or she considers that the disclosure of such information is necessary:

(a) to assist the foreign country in initiating or carrying out investigations or proceedings; or

(b) and might lead to a request for co-operation by the foreign country under this Act.

(2) Prior to providing such information, the Public Prosecutor may request that the information be kept confidential or only used subject to conditions.

60 Expedited preservation of stored computer data

(1) A foreign country may request or otherwise obtain an expedited preservation of data stored by means of a computer system, located within the territory of Vanuatu and in respect of which the requesting foreign country, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

(2) A request for expedited preservation made under subsection (1) must specify the following:

(a) the authority seeking the preservation; and

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

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

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

(e) the necessity of the expedited preservation; and

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

(3) Upon receiving a request under subsection (1), the Public Prosecutor must take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act.

(4) Any expedited preservation effected in response to the request is to be for a period not less than 60 days, in order to enable the foreign country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request, the data is to continue to be expedited preserved until a final decision is taken on that pending request.

(5) Subsections (1) and (2) must apply *mutatis mutandis* when a request for expedited preservation of stored computer data is done by Vanuatu.

61 Expedited disclosure of preserved traffic data

(1) In the course of executing a request under section 22 or otherwise in relation to a serious offence in a foreign country, the law enforcement agency, with respect to a specified communication, discovers that a service provider in another country is involved in the transmission of the communication, the Public Prosecutor is:

(a) to expeditiously disclose to the requesting foreign country a sufficient amount of traffic data to identify that service provider; and

(b) to disclose the path through which the communication was transmitted.

(2) Expedited disclosure of preserved traffic data under subsection (1) may only be withdrawn if:

(a) the request concerns a political offence or an offence related to a political offence; or

(b) the Public Prosecutor considers that the execution of the request is likely to prejudice Vanuatu's sovereignty, security or public interest.

62 Mutual assistance regarding accessing of stored computer data

(1) A foreign country may request to order or to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of Vanuatu, in relation to a foreign serious offence, including data that has been preserved pursuant to section 18.

(2) A request for mutual assistance regarding accessing of stored computer data is to, as far as practicable:

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

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

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

(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested country:

(i) give details of the offence in question; or

(ii) particulars of any investigation or proceeding commenced in respect of the offence,

and be accompanied by a copy of any relevant restraining or confiscation order; and

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

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

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

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

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

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

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

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

(3) Upon receiving the request under this section, the investigating agency must take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining necessary authorisation including any warrants to execute upon the request, the investigating agency may seek the support and cooperation of the foreign country during the search and seizure.

(5) Upon conducting the search and seizure request, the investigating agency must provide the results of such search and seizure to the foreign country.

(6) Subsections (1) and (2) must apply *mutatis mutandis* to requests for expedited preservation of stored computer data in the territory of a foreign country.

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

A police officer may, without the authorisation but subject to any applicable provisions of this Act:

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

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

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

(1) A foreign country may request, in relation to a foreign serious offence, to order or provide assistance in real-time collection of traffic data associated with specified communications in Vanuatu transmitted by means of a computer system.

(2) A request for assistance under this section is to specify:

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

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

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

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

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

(f) sufficient information to identify the traffic data; and

(g) any further details relevant traffic data; and

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

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

(3) Upon receiving a request under subsection (1), the investigating agency must take all appropriate measures to obtain the necessary authorisation, including any warrants to execute upon the request, in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining the necessary authorisation, including any warrants to execute upon the request, the investigating agency may seek the support and cooperation of the foreign country, during the search and seizure.

(5) Upon conducting the measures under this section, the investigating agency must provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the foreign country.

(6) Subsections (1) and (2) must apply *mutatis mutandis* to requests for real-time collection of traffic data in a foreign country.

65 Mutual assistance regarding the interception of content data

(1) A foreign country may request to order or otherwise provide assistance in the real-time collection, or recording of content data of specified communications transmitted by means of a computer system in Vanuatu.

(2) A request for assistance under subsection (1), so far as practicable, must specify:

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

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

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

(d) the location or the nature of the communication; and

(e) the intended purpose for the required communication; and

(f) sufficient information to identify the communications; and

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

(h) the recipient of the communication; and

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

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

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

(3) Upon receiving a request under this section, the Public Prosecutor must take all appropriate measures to execute upon the request in accordance with the procedures and powers provided under this Act.

(4) Upon conducting the measures under subsection (3), the Public Prosecutor must provide the results of such measures as well as real-time collection or recording of content data of specified communications to the foreign country.

(5) Subsections (1) and (2) must apply *mutatis mutandis* to requests for real-time collection of traffic data in a foreign country.

66 24/7 Network

(1) The Public Prosecutor must ensure that the investigating agency responsible for investigating and prosecuting cybercrime must designate a point of contact available on a twenty-four hour, seven-days-a-week basis.

(2) A designated point of contact under subsection (1), is to ensure assistance is immediately provided for the purpose of:

(a) investigations or proceedings concerning criminal offences related to computer systems and data; or

(b) for the collection of evidence in electronic form of a criminal offence,

which assistance is to include facilitating, or directly carrying out the following measures:

(i) the provision of technical advice; and

(ii) computer data and expedited disclosure of preserved traffic data; and

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

within expeditious timelines, as may be, prescribed by the Regulations.

(3) The point of contact is to be resourced with and possess the necessary capacity to securely and efficiently carry out communications with other points of contact in other territories, on an expedited basis.

(4) The point of contact is to have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.

67 Report on special investigative powers

(1) The Commissioner must, on or before the end of March of each year, submit an annual report to the Council of Ministers setting out general information and statistics relating to the use of special investigative powers for the previous year.

(2) The report must include to a minimum:

(a) the number of undercover operations authorised; and

(i) the number of orders issued to preserve computer data; and

(ii) the number of requests for traffic data in real time; and

(iii) the number of applications to produce computer data; and

(b) the number of applications for interception warrants and computer warrants; and

(c) the number of applications for renewals of interception warrants and computer warrants; and

(d) the number of applications for urgent interception warrants and urgent computer warrants; and

(e) the number of controlled deliveries of property authorised; and

(f) the number of applications referred to under paragraphs (b), (c) and (d) that were granted, and the number that were refused; and

(g) the number of prosecutions that have been instituted in which evidence obtained directly or indirectly from:

(i) an interception carried out pursuant to an interception warrant or urgent interception warrant; or

(ii) a data storage medium, computer network or computer system pursuant to a computer warrant or urgent computer warrant; or

(iii) an undercover operation; or

(iv) an order to preserve computer data; or

(v) a request to access to traffic data and traffic data in real time; or

(vi) an order to produce computer data; or

(vii) a controlled delivery of property has been adduced, and the result of those prosecutions; and

(viii) the number of interception warrants and computer warrants that did not result in any charges being laid within 90 days after the date on which the warrant expired; and

(ix) the number of undercover operations and controlled deliveries of property that did not result in any charges being laid within 90 days after the date on which the undercover operation or controlled delivery ended.

(3) Nothing in this section requires the Commissioner to publicly disclose the operational details of a particular case.

68 State not required to give undertaking for costs

Despite any other Act or law, Vanuatu is not required to give an undertaking for costs for applying for a warrant.

PART 6 MISCELLANEOUS

69 Authorised officer

(1) The Commissioner may appoint a police officer as an authorised officer to perform any functions or exercise any powers that may be performed or exercised for the purposes of this Act, for a period as may be determined by the Commissioner.

(2) The Commissioner is to provide to each authorised officer, an identity card that will provide evidence of the identity of that police officer and of the appointment of that police officer as an authorised officer.

(3) An authorised officer who holds an identity card issued under this section must, on the termination of his or her appointment, surrender the identity card to the Commissioner.

70 Protection from liability

(1) A police officer or authorised officer is not subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done by the police officer or authorised officer in good faith in the execution or purported execution of his or her powers and functions under this Act.

(2) A service provider or an authorised representative is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in performance of a duty imposed under this Act.

71 Regulations

The Minister may, make Regulations prescribing matters:

(a) required or permitted by this Act to be prescribed; or

(b) that are necessary or convenient to be prescribed for the better carrying out or giving effect to the provisions of this Act.

72 Commencement

This Act comes into force on the day on which it is published in the Gazette.