Tonga

COMPUTER CRIMES BILL 2019

COMPUTER CRIMES BILL 2019

Arrangement of Sections

Section

COMPUTER CRIMES BILL 2019

V01

A BILL FOR AN ACT TO PROVIDE FOR THE PREVENTION OF, INVESTIGATION, SUPPRESSION AND IMPOSITION OF PENALTIES OF COMPUTER-RELATED OFFENCES IN TONGA AND FOR RELATED PURPOSES

I assent,
TUPOU VI,
Date of Assent

Commencement [Date]

BE IT ENACTED by the King and Legislative Assembly of Tonga in the Legislature of the Kingdom as follows:

PART 1 PRELIMINARY

1 Short title and commencement

(1) This Act may be cited as the Computer Crimes Act 2019 .

(2) This Act comes into force on the date proclaimed by Cabinet.

2 Interpretation

In this Bill, unless the contrary intention is indicated:

"access" to computer data means:

(a) the display of the data by a computer system or any other output of the data from the computer system;

(b) the copying or moving of the data to another place in a computer system or to a data storage medium; or

(c) for a program—the execution of the program;

"authorised officer" means:

(a) a police officer who holds a rank of Sergeant or higher and is authorised in writing by the Police Commissioner; or

(b) for the purposes of Division 4.3 of this Act means an authorised officer under the Mutual Assistance in Criminal Matters Act.

"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;

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

"communications network" has the meaning given in section 2 (1) of the Communications Act ;

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

"computer system" means any device or a group of interconnected or related devices, one or more of which, in accordance with a program, performs automatic processing of data;

"content data" means data that forms the content or substance of a communication;

"Court" means the Supreme Court of Tonga;

"data" includes information in any form;

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

"electronic communication" means a communication of information or data in any form by way of guided or unguided electromagnetic energy;

"evidential material" means a thing relevant to an offence, including a thing in electronic form;

"foreign interception warrant" means a warrant issued under Division 4.3 in relation to access to and disclosure of content data;

"foreign preservation order" means an order under Division 4.3 requiring a service provider to retain specified traffic data or content data;

"foreign State" has the meaning given in section 3 (1) of the Mutual Assistance in Criminal Matters Act ;

"impairment" of electronic communication to or from a computer system:

(a) includes:

(i) the prevention of any electronic communication; and

(ii) the impairment of any electronic communication or network used by the computer system; but

(b) does not include a mere interception of any electronic communication;

"interception warrant" means a warrant issued under Subdivision 4.2.4 in relation to access to and disclosure of content data;

"Judge" means a Judge of the Supreme Court of Tonga;

"Minister" means the Minister responsible for communications;

"modification" of computer data means:

(a) the alteration or removal of the computer data; or

(b) an addition to the computer data;

"Police Commissioner" means the Commissioner of Tonga Police;

"preservation order" means an order under Subdivision 4.2.3 for the preservation of traffic data or content data;

"seize" or any variation of the word "seize" includes any of the following:

(a) making and retaining a copy of the computer data, including using on-site equipment;

(b) rendering inaccessible or removing the computer system;

(c) taking a printout of the data; or

(d) otherwise securing or maintaining the integrity of the computer data or computer system for later examination;

"serious offence" means an offence against a provision of:

(a) any law of Tonga, for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months or more severe penalty; or

(b) a law of a foreign State, in relation to acts or omissions which, had they occurred in Tonga, would have constituted an offence for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months, or more severe penalty, including an offence of a purely fiscal character.

"service" means a service provided by a service provider;

"service provider" means:

(a) a person that offers or provides services by means of a computer system or communications network;

(b) a person that offers or provides services that is accessible in Tonga;

(c) any other person that processes or stores data on behalf of a service provider or network operator; or

(d) a network operator under the Communications Act ;

"subscriber data":

(a) means any data not including traffic or content data, held by a service provider (whether in the form of computer data or any other form) in relation to a person using 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;

(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; or

(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;

"Tonga Police" has the meaning given in section 3 of the Tonga Police Act;

"traffic data" means :

(a) any computer data relating to an electronic communication that forms part of the chain of the communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

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

(c) any additional information relevant to the communication.

3 Jurisdiction

Unless otherwise provided for under this Act, proceedings may be brought for an offence under this Act:

(a) if the act or omission is committed:

(i) in Tonga;

(ii) on board a ship or aircraft registered in Tonga; or

(iii) by a person who is in Tonga; and

(b) whether or not the act or omission constituting the offence is committed in or outside Tonga, if the act or omission:

(i) is committed by a subject of Tonga or a citizen of any country who is ordinarily resident in Tonga;

(ii) is committed in order to compel the Government of Tonga to do or abstain from doing any act;

(iii) is committed against a subject of Tonga;

(iv) is committed by a person who is, after the commission of the offence, present in Tonga;

(v) is intended to be committed in Tonga; or

(vi) originates in or transits in Tonga.

PART 2 COMPUTER OFFENCES

DIVISION 2.1 INTERPRETATION

4 Limited meaning of "access to computer data" etc

In this part, a reference to:

(a) access to computer data;

(b) modification of computer data; or

(c) impairment of electronic communication to or from a computer system;

is limited to access, modification or impairment caused directly or indirectly by the execution of a function of a computer system.

5 Meaning of "unauthorised" access, modification or impairment

(1) For the purposes of this part, access to or modification of data, or impairment of electronic communication or of the reliability, security or operation of data, by a person is "unauthorised" if the person is not entitled to cause the access, modification or impairment.

(2) However, the access, modification or impairment is not unauthorised only because the person has an ulterior purpose for causing it.

DIVISION 2.2 COMPUTER OFFENCES GENERALLY

6 Unauthorised access to or modification of computer data

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

(a) causes unauthorised access to or modification of computer data;

(b) knows the access or modification is unauthorised; and

(c) intends to cause the access or modification.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $10,000, or imprisonment not exceeding 3 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $50,000.

7 Unauthorised access, modification or impairment with intent to commit serious offence

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

(a) causes:

(i) any unauthorised access to computer data;

(ii) any unauthorised modification of computer data; or

(iii) any unauthorised impairment of electronic communication to or from a computer system; and

(b) either:

(i) knows the access, modification or impairment is unauthorised; or

(ii) is reckless about whether the access, modification or impairment is unauthorised; and

(c) intends to commit, or enable the commission of, a serious offence by the person or by someone else.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $10,000, or imprisonment not exceeding 3 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $50,000.

(3) A person can be found guilty of an offence against this section:

(a) even if committing the serious offence is impossible; or

(b) whether the serious offence is to be committed at the time of the unauthorised conduct or at a later time.

8 Unauthorised modification of data in a computer system to cause impairment

(1) A person commits an offence if:

(a) the person causes unauthorised modification of computer data;

(b) the person knows the modification is unauthorised; and

(c) the person:

(i) intends by the modification to impair access to, or to impair the reliability, security or operation of, computer data;

(ii) causes such impairment; or

(iii) is reckless about any such impairment.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $100,000, or imprisonment not exceeding 10 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $200,000.

9 Unauthorised impairment of electronic communication

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

(a) causes unauthorised impairment of electronic communication to or from a computer system;

(b) knows the impairment is unauthorised; and

(c) either:

(i) intends to impair electronic communication to or from the computer system; or

(ii) is reckless about any such impairment.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $100,000,or imprisonment not exceeding 10 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $200,000.

10 Unauthorised impairment of data held in a data storage medium

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

(a) causes unauthorised impairment of the reliability, security or operation of data held in a data storage medium;

(b) knows the impairment is unauthorised; and

(c) intends to cause the impairment.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $50,000, or imprisonment not exceeding 7 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $100,000.

11 Unauthorised interception

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

(a) intercepts or causes the interception of communication data to, from or within a computer system or an electronic communication from a computer system that is holding computer data;

(b) knows the interception is unauthorised; and

(c) is reckless about whether the interception is unauthorised.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $100,000, or imprisonment not exceeding 10 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $200,000.

12 Possession of data with intent to commit or enable a computer offence

(1) A person commits an offence if the person has possession or control of data with the intention of committing or enabling an offence under this Part.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $10,000, or imprisonment not exceeding 3 year, or both; or

(b) in the case of a corporation, to a fine not exceeding $20,000.

(3) For the purposes of this section:

"possession or control of data" includes but not limited to the following:

(a) possession of a computer system or data storage medium holding data;

(b) possession of a document in which data is recorded;

(c) control of computer data that is in the possession of someone else (whether the computer system is in or outside Tonga); or

(d) possession or control of a password, access code or similar data that can be used to access a computer system;

(4) A person can be found guilty of an offence against this section even if committing the computer offence is impossible.

13 Producing, supplying, obtaining or otherwise making available data with intent to commit or enable a computer offence

(1) A person commits an offence if the person produces, supplies, obtains, or otherwise makes available, data with the intention of committing or enabling an offence under this Part.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $10,000, or imprisonment not exceeding 3 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $20,000.

(3) For the purposes of this section:

"produce, supply, obtain, or otherwise make available, data" includes but not limited to:

(a) produce, supply, obtain, or otherwise make available, data held in a computer system or data storage medium;

(b) produce, supply, obtain, or otherwise make available, a document in which data is recorded;

(c) produce, supply, obtain, or otherwise make available, a password, access code or similar data that can be used to access a computer system.

14 Unauthorised interference with a computer system

(1) A person commits an offence if:

(a) the person causes interference with:

(i) the functioning of a computer system; or

(ii) a person using or operating a computer system; and

(b) the interference is unauthorised; and

(c) the person either:

(i) knows the interference is unauthorised; or

(ii) is reckless about whether the interference is unauthorised.

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $100,000, or imprisonment not exceeding 10 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $200,000.

(3) For the purposes of this section, interference with the functioning of a computer system, or a person using or operating a computer system, by a person is **"unauthorised"** if the person is not entitled to interfere with the functioning of the computer system, or a person using or operating the computer system.

(4) In this section:

"interference", includes but not limited to the following:

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

(b) causing electromagnetic interference to the computer system;

(c) corrupting the computer system by any means.

PART 3 COMPUTER-RELATED OFFENCES

15 Using a communications network with intention to commit a serious offence

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

(a) connects equipment to a communications network;

(b) intends by this to commit, or to enable the commission of, a serious offence (by the person or by someone else).

(2) A person commits an offence if the person uses equipment connected to a communications network in the commission of, or to enable the commission of, a serious offence (by the person or by someone else).

(3) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $50,000, or imprisonment not exceeding 7 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $100,000.

16 Using a service to make a threat

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

(a) uses a service to make a threat to kill another person (the "other person") or a different person; and

(b) intends the other person to fear that the threat will be carried out.

(2) An offence against subsection (1) is punishable, on conviction to a fine not exceeding $100,000, or imprisonment not exceeding 10 years, or both.

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

(a) uses a service to make a threat to cause serious harm to another person (the "other person") or a different person; and

(b) intends the other person to fear that the threat will be carried out.

(4) An offence against subsection (3) is punishable, on conviction to a fine not exceeding $50,000, or imprisonment not exceeding 7 years, or both.

(5) In a prosecution for an offence against this section it is not necessary to prove that the person receiving the threat actually feared the threat would be carried out.

17 Using a service for a hoax threat

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

(a) uses a service; and

(b) does so with the intention of inducing a false belief that an explosive, or a dangerous or harmful substance or thing, has been or will be left in any place.

(2) An offence against subsection (1) is punishable, on conviction to a fine not exceeding $100,000, or imprisonment not exceeding 10 years, or both.

18 Using a service to menace, harass or cause harm

(1) In this section:

"intimate visual recording" includes but is not limited to:

(a) means a visual recording that is made in any medium using any device with or without the knowledge or consent of the person who is the subject of the recording, and that is of :

(i) a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the person is:

(A) naked or has the person's genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or

(B) engaged in an intimate sexual activity; or

(C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(ii) a person's naked or undergarment-clad genitals, pubic area, buttocks, or female breasts, which is made:

(A) from beneath or under a person's clothing; or

(B) through a person's outer clothing in circumstances where it is unreasonable to do so; and

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in:

(i) a physical form; or

(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing;

"post an electronic communication" includes but is not limited to:

(a) transfer, send, post, publish, disseminate, or otherwise communicate by means of electronic communication:

(i) any information, whether truthful or untruthful, about a person; or

(ii) an intimate visual recording of a person; and

(2) A person commits an offence if:

(a) the person uses a service or attempts to use a service to post an electronic communication;

(b) the person does so with the intention that the electronic communication be menacing, harassing or harmful to another person; and

(c) posting the electronic communication would be, in all the circumstances, menacing, harassing or harmful to a reasonable person in the other person's position.

(3) An offence against subsection (1) is punishable, on conviction, by imprisonment not exceeding 3 years. An offence against subsection (1) is punishable, on conviction to a fine not exceeding $10,000, or imprisonment not exceeding 3 years, or both.

(4) In determining whether a reasonable person would consider the posting of an electronic communication would cause harm to a person, the Court may take into account any factor it considers relevant, including the following:

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

(b) the person's age and characteristics;

(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;

(g) the context in which the communication was posted.

PART 4 PROCEDURAL POWERS

DIVISION 4.1 POWERS RELATING TO SEARCH WARRANTS ETC

19 Application for search warrant

(1) An authorised officer may apply to a Judge for a search warrant to search a person, or enter and search a place, if the authorised officer suspects on reasonable grounds that there may be on the person or at the place a computer system, computer data or data storage medium that:

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

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

(2) The application shall be supported by an affidavit sworn by an authorised officer and state the following:

(a) the authorised officer's name and rank;

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

(c) 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;

(d) the offence to which the application relates;

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

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

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

(ii) is likely to be on or under the control of the person or at the place when the search warrant is executed;

(g) whether a search warrant was issued previously in relation to the person or place;

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

(i) the period for which the warrant is required.

(3) The authorised officer shall provide, orally or in writing, any further information that the Judge requires.

(4) The authorised officer need not appear before the Judge when the Judge is considering the application.

20 Urgent application for search warrant

(1) An authorised officer may apply for a search warrant without a written application if:

(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 search warrant.

(2) The application may be made by electronic means.

(3) The application shall include:

(a) all information required to be provided in an application for a search warrant under section 19; and

(b) the reasons for making the application under this section.

(4) The authorised officer shall, as soon as practicable, send a copy of the application to the Judge.

21 Application to Magistrate if Judge unavailable

If a Judge is not available to hear an application under this Division for a search warrant, the Lord Chief Justice may appoint a Magistrate to hear the application.

22 Issue of search warrant

(1) If an application for a search warrant has been made under section 19 or section 20, the Judge may issue the warrant if satisfied that there are reasonable grounds for doing so.

(2) In deciding whether there are reasonable grounds for issuing a search warrant, the Judge shall consider the following:

(a) the seriousness of the offence;

(b) the credibility of the information on which the application is based;

(c) whether the public interest in a search being conducted under the warrant outweighs the right to privacy of a person whose privacy may be affected by the search;

(d) whether there is sufficient connection between the evidence sought and the offence to which the application relates;

(e) whether any condition should be imposed in relation to the execution of the warrant;

(f) in relation to an application under section 20, whether:

(i) a search warrant in the terms of the application should be issued urgently; or

(ii) the delay that would occur in making the application under section 19 would frustrate the effective execution of the search warrant;

(g) the proposed duration of the warrant; and

(h) any other matters the Judge considers relevant.

23 Search warrant issued following urgent application

(1) If a Judge issues a search warrant applied for under section 20, the Judge shall, as soon as practicable, give a copy of the search warrant to an authorised officer.

(2) If it is not reasonably practicable to give a copy of the warrant to an authorised officer:

(a) the Judge shall tell a authorised officer the terms of the search warrant and the date and time the warrant was signed; and

(b) the officer shall make a written record of the following details:

(i) the Judge's name;

(ii) the day and time the Judge signed the warrant;

(iii) the terms of the warrant.

(3) The authorised officer shall, send the Judge the sworn application within 48 hours.

24 What a search warrant shall state

(1) A search warrant shall state the following:

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

(b) if a place is to be searched:

(i) a description of the place that may be entered; and

(ii) whether the place may be entered at night;

(c) the offence to which the search warrant relates;

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

(e) the date and time the search warrant ends;

(f) that an authorised officer may exercise the search powers in section 26;

(g) any conditions imposed in relation to the execution of the search warrant.

(2) A search warrant issued under subsection (1) shall be deemed to:

(a) authorise the seizure of a thing that the authorised officer executing the warrant believes on reasonable grounds to be:

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

(ii) evidential material relevant to another offence under Tongan law; and

(b) a search of a person who is at or near the premises when the warrant is executed if the authorised officer executing the warrant suspects on reasonable grounds that the person has any evidential material in the person's possession.

(3) The search warrant shall also include the name and signature of the Judge issuing the warrant.

25 Extension of search warrant

(1) A Judge may extend the time and date when a search warrant ends if the Judge is satisfied that the purpose for which the search warrant was issued cannot be satisfied before the date and time stated in the warrant for the warrant's expiry.

(2) An extension shall:

(a) be made before the expiry of the search warrant;

(b) be made only once;

(c) not be for a period longer than 21 days; and

(d) be made by issuing an amended search warrant that states the new time and date the search warrant ends.

26 Search warrant powers

(1) An authorised officer executing a search warrant may do the following:

(a) enter the place named in the search warrant, or search the person named in the warrant, to:

(i) search a computer system, or part of it, or a data storage medium;

(ii) seize or secure the computer system, or part of it, or the data storage medium; and

(iii) search, seize, access and collate data held in the computer system or data storage medium;

(b) if the authorised officer believes on reasonable grounds that data on a computer system at the place or on the person, or data stored elsewhere that is accessible from that computer system, might be data that could be accessed, collated or seized under the warrant, the authorised officer may do any of the following:

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

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

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

(iv) seize the computer system and any data storage medium;

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

(c) move a computer system or data storage medium 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:

(i) if the occupier of the place consents; or

(ii) if:

(A) it is significantly more practicable to do so having regard to the time it will take to copy the data and the availability of the technical expertise required to do so; and

(B) there are reasonable grounds to suspect that the computer system or data storage medium contains data that could be accessed, collated or seized under the warrant;

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

(e) use other authorised officers or people as reasonably necessary for the execution of the warrant.

(2) A search of a person under a search warrant shall be conducted in accordance with section 143 and section 144 of the Tonga Police Act.

27 Access to data on seized computer system

(1) Subject to subsection (2), on request, an authorised officer or a person assisting an authorised officer executing a search warrant in relation to a place, shall:

(a) allow a person who had the custody or control of a computer system at the place, or someone acting on the person's behalf, to access and copy data held in the computer system; or

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

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

(a) constitute an offence; or

(b) prejudice:

(i) the investigation in relation to which the search was carried out;

(ii) another ongoing investigation; or

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

28 Securing etc computer system or data storage medium under search warrant

(1) An authorised officer executing a search warrant may do whatever is necessary to secure or render inaccessible a computer system or data storage medium that is on a person or at a place searched under the warrant if the authorised officer suspects on reasonable grounds that:

(a) evidence of the commission of an offence may be accessible by operating the computer system or data storage medium at the place where the person is searched or at the place searched;

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

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

(2) The authorised officer shall give notice to the person searched or the occupier of the place searched:

(a) of the authorised officer's intention to secure or render inaccessible the computer system or data storage medium; and

(b) that the system or medium may be secured or inaccessible for a period of up to 28 days.

(3) The computer system or data storage medium may be secured or inaccessible until whichever of the following happens first:

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

(b) the computer system or data storage has been operated by the expert.

(4) The authorised officer may apply to a Judge for an extension of the time mentioned in subsection (3) (a) if the authorised officer believes on reasonable grounds that the expert assistance will not be available within 28 days.

(5) More than one application may be made under subsection (4).

(6) The authorised officer shall give the person searched or the occupier of the place searched notice of the authorised officer's intention to apply for an extension, and that the person or occupier is entitled to be heard in relation to the application.

29 Assisting police in executing search warrant

(1) Subsection (2) applies if an authorised officer executing a search warrant in relation to a person or place specified in the warrant suspects on reasonable grounds that computer data held on, or accessible from a computer system or data storage medium on the person or at the place might be data that could be accessed, collated or seized under the warrant.

(2) The authorised officer may direct the person searched or, if a place is searched, a person in possession or control of, or with knowledge of, the computer system or data storage medium to give reasonable assistance to the authorised officer to:

(a) access and operate the computer system or data storage medium to access any computer data (including data stored on a separate data storage medium or data not held on the person or stored at the place);

(b) operate a computer system accessible from a computer system operated under paragraph (a) to access any computer data (including data stored on a separate data storage medium or data not held on the person or stored at the place);

(c) obtain and copy the data;

(d) use equipment to make copies of the data;

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

(f) do anything else the authorised officer reasonably requires.

(3) A person who fails without reasonable excuse to comply with a direction under subsection (2) commits an offence.

(4) An offence against subsection (3) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $10,000, or imprisonment not exceeding 3 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $20,000.

30 Examination not to cause damage

(1) This section applies if a search warrant authorises an authorised officer executing the warrant to do something mentioned in section 26(1)(b) or section 29.

(2) The authorised officer shall not exercise a power mentioned in section 26(1)(b) or section 29 unless the authorised officer, or any other person assisting the authorised officer, believes on reasonable grounds that the examination can be carried out without damaging the computer system or data storage medium or data.

31 Receipt for things seized under search warrant

(1) If a search warrant authorises an authorised officer to seize something, the authorised officer shall, as soon as reasonably practicable after seizing the thing:

(a) if a person is searched or a place searched is occupied—give, or cause to be given to, the person searched or occupier of the place searched a receipt for the thing seized; or

(b) if a place searched is not occupied—leave a receipt for the thing seized in a conspicuous place at the place searched.

(2) The receipt shall contain sufficient information to identify the things seized.

32 Returning computer system or data storage medium

(1) A computer system or data storage medium moved under a search warrant shall be returned to either of the following people when it is no longer required for the investigation or prosecution of an offence:

(a) if the computer system or data storage medium was removed from a person—that person;

(b) if the computer system or data storage medium was removed from a place—the owner or occupier of that place.

(2) A computer system or data storage medium shall not be returned to a person or a place mentioned in subsection (1) if an authorised officer believes on reasonable grounds that:

(a) it was appropriate for the computer system or data storage medium to be seized under the search warrant; or

(b) possession of data on the computer system or data storage medium may constitute an offence.

33 Minimising need to retain seized computer system or data storage medium

(1) An authorised officer who seizes a computer system or a data storage medium under a search warrant shall take the steps reasonably necessary to minimise the need to retain the computer system or data storage medium as evidence by doing any of the following as soon as practicable:

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

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

(c) gathering any other available secondary evidence in relation to the system or medium.

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

34 Retained computer system or data storage medium—exercising reasonable care

An authorised officer, or a person assisting the authorised officer, who retains a computer system or a data storage medium seized under a search warrant shall take reasonable care to prevent any damage to the following:

(a) the computer system or data storage medium;

(b) data stored on the computer system or data storage medium;

(c) data accessed by operating the computer system or data storage medium;

(d) programs associated with the use of the computer system or data storage , or with the use of the data stored on the computer system or data storage medium.

35 Destruction of certain data under a warrant

If the Police Commissioner is satisfied that data accessed or copied under a search warrant is no longer useful for the investigation or prosecution of an offence, the Police Commissioner shall arrange for the destruction of the data from any computer system or data storage medium, and any other reproduction of the data, under the control of the Tonga Police.

36 Preservation of data held in computer system

(1) Subsection (2) applies if an authorised officer is satisfied on reasonable grounds that:

(a) data held in a computer system is required for the purpose of a criminal investigation or proceeding; and

(b) there is a risk that the data may be destroyed or rendered inaccessible.

(2) The authorised officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice is preserved for a period of up to 90 days.

(3) The authorised officer may apply to the Police Commissioner for an extension of the time for a period of not more than 90 days mentioned in subsection (2).

(4) More than one application may be made under subsection (3).

(5) A person issued with a notice under subsection (2) shall maintain the confidentiality of any procedures and information relating to the notice while the notice is in force.

(6) A person who fails, without reasonable excuse, to comply with subsection (5) commits an offence punishable, on conviction, to a fine not exceeding $20,000.

37 Production of data held in a computer system

(1) This section applies if an authorised officer makes an application to a Judge that specified data held in a computer system, or a printout or other information, is reasonably required for the purpose of a criminal investigation or proceeding.

(2) The Judge may order:

(a) a person in control of the computer system to produce from the computer system, data or a printout or other intelligible output of that data; and

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

(3) Before making an order under subsection (2), the Judge shall consider the following:

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

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

(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;

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

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

(f) any other matters that the Judge considers relevant.

38 Purposes for which things, documents and data may be used

(1) An authorised officer may use, or make available for use, or disclose, any of the following, only for the purpose of preventing, investigating or prosecuting an offence:

(a) a thing seized under this Division;

(b) a document, or a copy of a document, produced under this Division;

(c) a computer system or data storage medium, including any data extracted from the computer system or data storage medium, moved for examination under this Division;

(d) private information about another person obtained during the exercise of police powers under this Division.

(2) Subsection (1) also applies to making a thing, document, data or information available for use by a foreign law enforcement agency in accordance with this Division and the Mutual Assistance in Criminal Matters Act.

39 Offence—hindering or obstructing search

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

(a) hinders or obstructs an authorised officer, or a person assisting an authorised officer, in carrying out a search of a person or place under this Division; and

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

(2) An offence against subsection (1) is punishable, on conviction:

(a) in the case of an individual, to a fine not exceeding $50,000, or imprisonment not exceeding 7 years, or both; or

(b) in the case of a corporation, to a fine not exceeding $100,000.

DIVISION 4.2 SPECIFIC PROVISIONS APPLYING TO SERVICE PROVIDERS

SUBDIVISION 4.2.1 DISCLOSURE OF SUBSCRIBER DATA

40 Request for disclosure of subscriber data

(1) An authorised officer may, in writing, ask a service provider to disclose subscriber data if the disclosure is reasonably necessary:

(a) for law enforcement purposes;

(b) to enforce the criminal law;

(c) to enforce a law imposing a pecuniary penalty;

(d) to protect the public revenue; or

(e) for national security purposes.

(2) Before making a request under subsection (1), the authorised officer shall be satisfied that the public interest in the disclosure of the subscriber data is reasonably necessary.

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

41 Subscriber data to be used for lawful purposes only

(1) Subscriber data disclosed under section 40 may only be used:

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

(b) for law enforcement purposes;

(c) to enforce the criminal law;

(d) to enforce a law imposing a pecuniary penalty;

(e) to protect the public revenue; or

(f) for national security purposes.

(2) If the authorised officer requesting the disclosure is satisfied that data obtained under section 40 is no longer useful for a purpose mentioned in subsection (1), the authorised officer shall arrange for the destruction of the data and any reproduction of the data in the control of the Tonga Police.

SUBDIVISION 4.2.2 ACCESS TO AND DISCLOSURE OF TRAFFIC DATA

42 Request for disclosure of traffic data

(1) An authorised officer may, in writing, request a service provider to disclose records of traffic data if the disclosure is reasonably necessary:

(a) for law enforcement purposes;

(b) to enforce the criminal law;

(c) to enforce a law imposing a pecuniary penalty;

(d) to protect the public revenue; or

(e) for national security purposes.

(2) Before making a request under subsection (1), the authorised officer shall:

(a) be satisfied that the public interest in the disclosure of the data 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 making the request, including the following:

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

(ii) the gravity of the conduct being investigated;

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

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

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

43 Request for access to traffic data in real time

(1) The Police Commissioner or a Deputy Police Commissioner authorised by the Police Commissioner, may in writing request a service provider to provide access to records of traffic data in real time if the access is reasonably necessary for the enforcement of an offence punishable, on conviction, by imprisonment for at least 3 years.

(2) Before making a request under subsection (1), the Police Commissioner or a Deputy Police Commissioner:

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

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

(ii) the gravity of the conduct being investigated;

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

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

44 When request to access traffic data in real time comes into force

(1) A request to a service provider under section 43 (1):

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

(b) ceases to be in force on whichever of the following dates happens first:

(i) the date specified by the Police Commissioner or a Deputy Police Commissioner (not more than 45 days after the request comes into force); or

(ii) the date the request is revoked by the Police Commissioner or a Deputy Police Commissioner.

45 Revocation of request to access traffic data in real time

(1) The Police Commissioner or a Deputy Police Commissioner authorised by the Police Commissioner may, in writing revoke a request under section 43 (1) any time before it ends.

(2) The Police Commissioner or a Deputy Police Commissioner shall revoke the request in writing, if the Commissioner is satisfied the request is no longer required.

(3) If the request is revoked, the Police Commissioner or a Deputy Police Commissioner shall tell the service provider's authorised representative about the revocation, and give the representative a copy of the revocation, as soon as practicable.

46 Traffic data to be used for lawful purposes only

(1) Traffic data disclosed or accessed under this Division may only be used:

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

(b) law enforcement purposes;

(c) to enforce the criminal law;

(d) to enforce a law imposing a pecuniary penalty;

(e) to protect the public revenue; or

(f) for national security purposes

(2) If the Police Commissioner is satisfied that data obtained under section 42 or section 43 is no longer useful for a purpose mentioned in subsection (1), the Commissioner shall arrange for the destruction of any record in the control of the Tonga Police.

SUBDIVISION 4.2.3 PRESERVATION ORDERS

47 Preservation of traffic or content data

The authorised officer may issue a service provider with a preservation order to preserve specified traffic data or content data.

The authorised officer may only issue a preservation order if satisfied on reasonable grounds that the preservation of the traffic or content data is reasonably necessary:

(a) for law enforcement purposes;

(b) to enforce the criminal law;

(c) to enforce a law imposing a pecuniary penalty;

(d) to protect the public revenue; or

(e) for national security purposes.

(3) A service provider issued with a preservation order shall disclose, as soon as practicable, a sufficient amount of traffic data to enable the authorised officer to identify any other service providers involved in the transmission of the communication.

48 When preservation order in force

(1) A preservation order:

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

(b) remains in force -

(i) for the period stated in the order (for a period of up to 90 days); or

(ii) until revoked by the authorised officer.

(2) The authorised officer may extend the period for which a preservation order is in force by up to 90 days.

(3) The authorised officer may extend the period more than once.

49 Revocation of preservation order

(1) The authorised officer may, in writing, revoke a preservation order any time before it ceases to be in force.

(2) The authorised officer shall revoke a preservation order if they are satisfied the order is not required.

(3) If a preservation order is revoked, the authorised officer shall tell the service provider's authorised representative about the revocation, and give the authorised representative a copy of the revocation, as soon as practicable.

SUBDIVISION 4.2.4 INTERCEPTION WARRANTS

50 Application for interception warrant

(1) An authorised officer may apply to the Court for a warrant to intercept one or more services to allow access to and disclosure of content data in relation to:

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

(i) an offence against section 6,12,13,15 and18; or

(ii) an offence punishable, on conviction, by imprisonment for at least 5 years; and

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

(2) The application shall be sworn by the authorised officer and state the following:

(a) the authorised officer's name, rank and station;

(b) details of each service provider to whom the warrant applies, if those details are known;

(c) the offence or offences to which the application relates;

(d) the information or evidence relied upon ;

(e) the extent to which other methods for the investigation of the offence have been used or are available;

(f) whether a preservation order has been issued;

(g) whether an interception warrant was previously issued for the same matter.

(3) The authorised officer shall provide, orally or in writing, any further information the Court requires concerning the grounds on which the interception warrant is sought.

(4) The authorised officer need not appear before the Court when the Court is considering the application unless the Court reasonably requires it.

51 Urgent application for interception warrant

(1) An authorised officer may apply to the Court for an interception warrant without a sworn written application if:

(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) The application may be made by electronic means.

(3) The application shall include:

(a) all information required to be provided in an application for an interception warrant under section 50; and

(b) the reasons for making the application under this section.

(4) The authorised officer shall, send a copy of the application to the Court within 48 hours after being granted the interception warrant.

52 Consideration of application for interception warrant

(1) If an application for an interception warrant is made under section 50 or section 51, the Court may issue the warrant for the interception of one or more of the following if satisfied there are reasonable grounds for doing so:

(a) content data in its passage over a communications network;

(b) content data in a stored form;

(c) content data preserved under a preservation order.

(2) In deciding whether there are reasonable grounds for issuing an interception warrant, the Court shall:

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

(b) be satisfied that the person mentioned in section 50 (1) has used, is using or is likely to use the service mentioned in that section or is likely to use more than 1 service; and

(c) be satisfied in relation to the matters mentioned in section 50 (2) (d) to (g); and

(d) in relation to an application under section 51, be satisfied:

(i) that an interception warrant in the terms of the application should be issued urgently; or

(ii) the delay that would occur in making the application under section 50 would frustrate the effective execution of the interception warrant; and

(e) consider relevant matters, including the following:

(i) the nature of the data to be disclosed;

(ii) the gravity of the conduct being investigated;

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

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

(v) whether other methods for the investigation of the offence have been used or are available;

(vi) whether any conditions should be imposed in relation to the execution of the interception warrant.

53 Form and content of interception warrant

(1) An interception warrant issued under section 52 shall be in the form prescribed by regulation.

(2) The warrant shall be in the prescribed form and signed by a Judge

(3) A warrant may specify conditions or restrictions relating to the interception under the warrant

(4) A warrant shall specify the period for which it is to be in force, being a period of up to 90 days.

(5) A Judge shall not vary a warrant by extending the time it is in force.

54 Interception warrant issued following urgent application

(1) If the Court issues an interception warrant applied for under section 51, the Court shall, as soon as practicable, give a copy of the warrant to an authorised officer.

(2) If it is not reasonably practicable to give a copy of the interception warrant to an authorised officer:

(a) the Court shall tell an authorised officer the terms of the warrant and the date and time the warrant was signed; and

(b) the officer shall record on a prescribed form the following details:

(i) the name of the Judge who issued the warrant;

(ii) the date and time the warrant was signed;

(iii) the terms of the warrant.

55 Service provider to be served with interception warrant

(1) If an interception warrant is issued under this Division, the authorised officer to whom the warrant is issued shall:

(a) immediately tell the service provider's authorised representative about the issue of the warrant; and

(b) as soon as practicable, give the authorised representative a copy of:

(i) the interception warrant; or

(ii) the form completed by the officer under section 54(2)(b).

(2) The service provider shall comply with the requirements of the warrant forthwith.

56 Content data to be used for lawful purpose only

(1) The content data disclosed under an interception warrant served under section 55 may only be used—

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

(b) to enforce an offence mentioned in subsection 50 (1); or

(c) for a purpose under the Mutual Assistance in Criminal Matters Act .

(2) If the Police Commissioner is satisfied that any data obtained under sub-section (1) is no longer useful for a purpose mentioned in subsection (1), the Commissioner shall arrange for the destruction of any data in the control of the Tonga Police.

57 Revocation of interception warrant

(1) An authorised officer may, at any time, apply to the Court to revoke an interception warrant.

(2) The Court shall revoke an interception warrant if satisfied that the access or disclosure of the content data is no longer required.

(3) If an interception warrant is revoked, the authorised officer shall immediately tell the service provider's authorised representative about the revocation, and provide a copy of the revocation as soon as practicable.

DIVISION 4.3 ASSISTANCE TO FOREIGN STATES

58 Request for foreign preservation order

(1) A foreign State may, request the Attorney General to arrange for a service provider to preserve content or traffic data.

(2) If a request under sub-section (1) is to be followed by a request under the Mutual Assistance in Criminal Matters Act, the request for the preservation shall be in writing and include the following:

(a) the name of the authority making the request from the foreign State;

(b) the criminal offence ;

(c) the name of the law enforcement agency in the foreign State concerned with the criminal matter;

(d) information about the traffic or content data to be preserved and the relationship of the data to the offence;

(e) if possible, the identity of the service provider;

(f) the reasons for the request;

(g) a statement to the effect that the foreign State intends to make a formal request under the Mutual Assistance in Criminal Matters Act for access to the data to be preserved under the foreign preservation order.

59 Issuing a foreign preservation order

(1) If a foreign State requests a foreign preservation order under section 58 for the preservation of traffic or content data, the Attorney General shall issue a foreign preservation order to a service provider if satisfied that:

(a) the foreign State intends to make a formal request for mutual assistance under the Mutual Assistance in Criminal Matters Act for access to content and traffic data to be preserved under the foreign preservation order; and

(b) either:

(i) for a request for traffic data—the request relates to a criminal investigation or proceeding involving a serious offence against the law of the foreign State; or

(ii) for a request for content data—the request relates to a criminal investigation or proceeding involving an offence against the law of the foreign State punishable, on conviction, by imprisonment for at least 5 years; and

(c) the execution of the request is not likely to prejudice Tonga's sovereignty, security or public order or other essential interests.

(2) A service provider issued with a foreign preservation order shall disclose, as soon as practicable, a sufficient amount of traffic data to enable the Attorney General to identify any other service providers involved in the transmission of the communication.

(3) If, from the information provided under subsection (2), the Attorney General discovers that a service provider in another country was involved in the transmission of the communication, the Attorney General shall disclose to the foreign State a sufficient amount of traffic data to enable the foreign State to identify the foreign service provider.

(4) Disclosure of traffic data under subsection (3) may be withheld if the Attorney General considers that the disclosure is likely to prejudice Tonga's sovereignty, security or public order or other essential interests.

(5) In this section:

"political offence" has the meaning given in section 4 (4) of the Mutual Assistance in Criminal Matters Act .

60 When foreign preservation order in force

(1) A foreign preservation order:

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

(b) remains in force—

(i) for the period stated in the order (for a period of up to90 days); or

(ii) until revoked by the Attorney General.

(2) The Attorney General may extend the period for which a preservation order is in force by up to 90 days.

(3) The Attorney General may extend the period more than once.

61 Disclosure under foreign preservation order

(1) Traffic data or content data preserved under a foreign preservation order may only be disclosed in accordance with:

(a) section 70; and

(b) the Mutual Assistance in Criminal Matters Act.

62 Revocation of foreign preservation order

(1) This section applies if:

(a) a foreign preservation order is made in relation to a foreign State; and

(b) any of the following events happens:

(i) the Attorney General refuses a request by the foreign State under the Mutual Assistance in Criminal Matters Act for access to the traffic or content data preserved under the foreign preservation order;

(ii) the foreign State withdraws a request under the Mutual Assistance in Criminal Matters Act for access to the traffic or content data preserved under the foreign preservation order;

(iii) the foreign State fails to make a request under section 63 or under the Mutual Assistance in Criminal Matters Act within a reasonable time after a service provider receives the order.

(2) The Attorney General shall, in writing, revoke the foreign preservation order as soon as practicable after an event mentioned in subsection (1) happens.

(3) If the Attorney General revokes the foreign preservation order, the Attorney General shall tell the service provider's authorised representative about the revocation, and give the authorised representative a copy of the revocation, immediately after the order is revoked.

63 Request by foreign State for disclosure of traffic data

(1) If a foreign State makes a request under section 4 (2) of the Mutual Assistance in Criminal Matters Act for the disclosure of traffic data, the Attorney General may request the service provider to give the Attorney General the traffic data for disclosure.

(2) Before making the request, the Attorney General shall:

(a) be satisfied that the disclosure is reasonably necessary for the enforcement of a serious offence against the law of the foreign State requesting the disclosure; and

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

(c) consider relevant matters, including the following:

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

(ii) the gravity of the conduct being investigated;

(iii) whether there are reasonable grounds to believe the disclosure is relevant to that investigation;

(iv) the purpose for which access to the records is requested as part of that investigation.

(3) A service provider shall comply with a request under subsection (1) as soon as practicable after it is made.

(4) This section does not apply to traffic data in real time.

64 Request for access to traffic data in real time

(1) This section applies if the Attorney General receives a request for access to records of traffic data in real time from a foreign State under section 4 (2) of the Mutual Assistance in Criminal Matters Act.

(2) The Attorney General may request a service provider to provide access to the records mentioned in subsection (1) if the Attorney General:

(a) is satisfied in all the circumstances that the access is reasonably necessary for the investigation of an offence against a law of the foreign State that:

(i) is punishable, on conviction, by imprisonment for at least 3 years; or

(ii) involves an act or omission that, if it had happened in Tonga, would have constituted an offence punishable, on conviction, by imprisonment for at least 3 years; and

(b) is satisfied in relation to the things mentioned in section 63 (2).

(3) The service provider shall comply with a request under subsection (2) as soon as practicable after it is made.

65 When request for access to traffic data in real time in force

(1) A request to a service provider under section 64 to provide access to traffic data in real time:

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

(b) ceases to be in force on whichever of the following happens first:

(i) the date the request is revoked under section 66;

(ii) the time specified by the Attorney General.

(2) The time specified by the Attorney General under subsection (1) (b) (ii) shall not be longer than 21 days, beginning on the day the request comes into force.

(3) The Attorney General may extend the time under subsection (1) (b) (ii) once only for a further 21 days.

66 Revocation of request for access to traffic data in real time

(1) The Attorney General may, in writing, revoke a request under section 64 at any time.

(2) The Attorney General shall revoke a request under section 64 if satisfied that the access to or disclosure of the traffic data in real time is no longer required.

(3) If a request under section 64 is revoked, the Attorney General shall tell the service provider's authorised representative about the revocation, and give the authorised representative a copy of the revocation, immediately after the request is revoked.

67 Request by foreign State for disclosure of stored content data

If a foreign State makes a request under section 4 (2) of the Mutual Assistance in Criminal Matters Act for disclosure of the following content data, the Attorney General may apply for a foreign interception warrant for the disclosure of either or both of the following:

(a) content data in a stored form;

(b) content data preserved under a foreign preservation order.

68 Application for foreign interception warrant

(1) The Attorney General may apply to the Court for a foreign interception warrant to require a service provider to allow access to and disclosure of content data

for a request under section 4 (2) of the Mutual Assistance in Criminal Matters Act in relation to:

(a) a person engaged in, or suspected on reasonable grounds to be engaged in, the commission of an offence punishable, on conviction, by at least 5 years imprisonment; and

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

(2) The application shall be supported by an affidavit sworn by the Attorney General or an authorised officer and state the following:

(a) details of each service provider to whom the warrant applies, if those details are known;

(b) the offence to which the application relates;

(c) the information or evidence relied on to support a suspicion that the content data is held or transmitted by each service provider to whom the warrant applies;

(d) whether a preservation order has been issued in relation to a service used by the person to whom the warrant applies and whether access to data preserved under the order is sought under the warrant.

(3) The Attorney General or an authorised officer shall provide, orally or in writing, any further information the Court requires concerning the grounds on which the interception warrant is sought.

69 Consideration of application for foreign interception warrant

(1) If an application for a foreign interception warrant is made under section 68, the Court may issue the warrant for the interception of either or both of the following if satisfied there are reasonable grounds for doing so:

(a) content data in a stored form;

(b) content data preserved under a foreign preservation order.

(2) In deciding whether there are reasonable grounds for issuing a foreign interception warrant, the Court shall:

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

(b) be satisfied that the person mentioned in section 68 (1) has used, is using or is likely to use the service mentioned in that section or is likely to use more than one service; and

(c) be satisfied in relation to the matters mentioned in section 68 (2) (c) and (d); and

(d) consider relevant matters, including the following:

(i) the nature of the data to be disclosed;

(ii) the gravity of the conduct being investigated;

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

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

(v) whether any conditions should be imposed in relation to the execution of the interception warrant.

70 Disclosing data to foreign State

(1) This section applies if the Attorney General receives a request from a foreign State under section 4 (2) of the Mutual Assistance in Criminal Matters Act for disclosure of:

(a) traffic data; or

(b) traffic data in real time; or

(c) content data under a foreign interception warrant.

(2) The Attorney General may only disclose data to the foreign State on the following conditions:

(a) the data is used only for the purposes for which the foreign State requested it, unless the Attorney General gives written permission to use the data for the enforcement of a serious offence against the law of the foreign State;

(b) any document or other thing containing the data will be destroyed when it is no longer required for those purposes;

(c) any other condition determined, in writing, by the Attorney General.

DIVISION 4.4 EVIDENTIARY CERTIFICATES

71 Evidentiary certificates—service providers

(1) An authorised representative of a service provider may issue an evidentiary certificate sworn by the representative setting out the facts that the authorised representative considers relevant in relation to:

(a) acts or things done by a representative of the service provider in connection with, or in relation to :

(i) comply with a request to access traffic data in real time; or

(ii) comply with a preservation order; or

(iii) enable an interception warrant to be executed.

(2) An evidentiary certificate issued under subsection (1) shall be received into evidence in the proceeding without further proof and is conclusive evidence of the matters stated in it.

72 Evidentiary certificates—Police Commissioner

(1) The Police Commissioner or a Deputy Police Commissioner authorised by the Police Commissioner, may issue an evidentiary certificate sworn by them setting out the facts that the Commissioner or Deputy Police Commissioner considers relevant in relation to:

(a) acts or things done by a Police Commissioner or a Deputy Police Commissioner authorised by the Police Commissioner or an authorised officer in connection with the making or execution of any of the following:

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

(ii) a preservation order; or

(iii) an interception warrant; or

(b) anything done by a person in connection with:

(i) the communication to another person of information obtained under an order, request or warrant mentioned in paragraph (a); or

(ii) the making use of the information; or

(iii) the making of a record of the information; or

(iv) the custody of a record of the information; or

(v) the giving in evidence of the information.

(2) An evidentiary certificate issued under subsection (1) shall be received into evidence in the proceeding without further proof is prima facie evidence of the matters stated in it.

A document certified in writing by an authorised officer to be a true copy of a warrant shall be received in evidence as if it were the original warrant.

DIVISION 4.5 OBLIGATIONS OF SERVICE PROVIDERS

73 Obligations of service providers

(1) A service provider shall do its best to prevent communications networks and facilities from being used in, or in relation to, the commission of offences against the laws of Tonga.

(2) A service provider shall give Tonga Police such assistance as is reasonably necessary for the following purposes:

(a) for law enforcement purposes;

(b) to enforce the criminal law;

(c) to enforce a law imposing a pecuniary penalty;

(d) to protect the public revenue; or

(e) for national security purposes.

(3) A service provider 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 by subsection (1) or (2).

(4) An authorized representative, employee or agent of a service provider 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 connection with an act done or omitted by the provider as mentioned in subsection (3).

(5) A service provider who receives a request for information under this Act shall maintain the confidentiality of any procedures and information relating to the request.

(6) A service provider who fails, without reasonable excuse, to comply with subsection (5) commits an offence punishable, on conviction, to a fine not exceeding $20,000.

(7) A service provider commits an offence if the service provider fails to comply with a request under Division 4.2 or Division 4.3.

(8) An offence under subsection (7) is punishable, on conviction, to a fine not exceeding $100,000.

(9) A reference in this section to giving assistance includes, but is not limited to:

(a) the provision of services in executing an interception warrant under this Act; or

(b) providing relevant information about:

(i) any communication that is lawfully intercepted under an interception warrant; or

(ii) any communication that is lawfully accessed under an interception warrant; or

(c) complying with a preservation notice or a foreign preservation notice that is in force under Part 4; or

(d) disclosing subscriber or traffic data in accordance with this Act; or

(e) any other reasonably necessary assistance.

74 Terms and conditions on which assistance is to be given

(1) This section applies if a service provider is required to give assistance to Tonga Police as mentioned in section 73 (2).

(2) The service provider shall comply with the requirement on the basis that the provider neither profits from, nor bears the costs of, giving that assistance.

(3) The service provider shall comply with the requirement on such terms and conditions as are agreed between the service provider and the Tonga Police.

PART 5 MISCELLANEOUS

75 Authorised officer may seek assistance

(1) An authorised officer exercising a power under this Act may request another person to assist the authorised officer in the exercise of that power.

(2) A person requested by an authorised officer for assistance in the exercise of a power under this Act shall give the authorised officer the reasonable assistance necessary for the exercise of those powers.

76 Regulations

The Minister responsible may make regulations for the proper and efficient administration of this Act.

77 Transitional arrangements

The Minister responsible may make regulations under section 76 dealing with transitional arrangements.

78 Repeal

The Computer Crimes Act is hereby repealed.

Note: Under section 15 of the Interpretation Act, the repeal of the Computer Crimes Act does not affect:

(a) the past operation of or anything done or suffered under that Act

(b) any offence committed, or any right, liberty, obligation or penalty acquired or incurred under that Act any action, proceeding, or thing pending or incomplete when this Act comes into operation, but every such action, proceeding or thing may be carried on and completed as if that Act had not been repealed.

EXPLANATORY NOTES

(These notes do not form part of the Bill and are only intended to explain its scope and purpose)

The purpose of this Bill is to repeal and replace the Computer Crimes Act and fulfil Tonga's obligation as a Party to the Council of Europe Convention on Cybercrime ("Convention") which Tonga acceded to in May 2017. As a requirement of being Party to the Convention, Tonga's legislation must be compliant with the Articles of the Convention. The main objective of the Convention is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

An Explanatory Report, prepared by the Council of Europe, accompanies the Convention. Where this Bill is implementing an obligation under the Convention, the Bill should be interpreted as operating in a way consistent with the Convention. In doing so, the Explanatory Report may be valuable in interpreting this Bill.

The Bill consists of 78 extensive provisions which are divided into five Parts. These Parts cover interpretation, computer offences, computer related offences, procedural powers and miscellaneous provisions. The Bill also has consequential amendments to the Copyright Act, Criminal Offences Act, Interpretation Act and the Tonga Police Act.

PART 1 PRELIMINARY

Section 1 is a formal provision specifying the short title of the Bill. It provides that the Bill comes into force on the date proclaimed by Cabinet.

Section 2 defines the terms access, authorised officer, authorised representative, communications network, computer data, computer system, content data, Court, data, data storage medium, electronic communication, evidential material, foreign interception warrant, foreign preservation order, foreign State, impairment, interception warrant, Judge, modification, Police Commissioner, preservation order, seize or any variation of the word seize, serious offence, service, service provider, subscriber data, Tonga Police and traffic data on which the procedural powers will rely.

Section 3 provides for jurisdiction for this Bill. This implements Article 22 under the Convention.

PART 2 COMPUTER OFFENCES

This Part of the Bill covers the computer offences provisions and other related provisions in the area of computer crimes. The intentions of these provisions is to protect the confidentiality, integrity, and availability of a computer system or data and not to criminalise legitimate and common activities or practices. There are two Divisions in this Part namely Division 2.1 which covers Interpretation and Division 2.2 which covers computer offences generally. This implements Article 2 to Article 13 under the Convention.

DIVISION 2.1 INTERPRETATION

Section 4 provides for the limited meaning of "access to computer data" etc. An example of this is when computer data may be accessed by printing the data, or copying or moving the data to another place in the computer system or a data storage medium.

Section 5 provides for the meaning of "unauthorised" access, modification or impairment.

DIVISION 2.2 COMPUTER OFFENCES GENERALLY

The provisions under this Division covers the criminalization and sanctioning of unauthorised actions committed by a person in different forms on and through a computer system. It is important to note authorised acts by person, which is done for various purposes, under this Division are not criminalized.

Section 6 criminalizes and sanctions unauthorised access or modification of computer data.

Section 7 criminalizes and sanctions unauthorised access, modification or impairment with intent to commit a serious offence.

Section 8 criminalizes and sanctions unauthorised modification of data in a computer system to cause impairment.

Section 9 criminalizes and sanctions unauthorised impairment of electronic communication.

Section 10 criminalizes and sanctions unauthorised impairment of data held in a data storage medium.

Section 11 criminalizes and sanctions unauthorised interception.

Section 12 criminalizes and sanctions possession of data with intent to commit or enable a computer offence.

Section 13 criminalizes and sanctions producing, supplying, obtaining or otherwise making available data with intent to commit or enable a computer offence. This section also makes reference to the terms "produce, supply, obtain, or otherwise make available, data" and its interpretation in this section.

Section 14 criminalizes and sanctions unauthorised interference with a computer system. This section also makes reference to the terms "unauthorised" and "interference" and its interpretation in this section.

PART 3 COMPUTER-RELATED OFFENCES

This Part of the Bill covers the criminalization and sanction provisions and other related provisions in the area of computer related crimes. The intention of these provisions is to protect individuals from offences that are facilitated by and through a computer system. The provisions in this Part also include acts that are committed using mobile devices or through a post on social media.

Section 15 criminalizes and sanctions the using of a communications network with intention to commit a serious offence.

Section 16 criminalizes and sanctions the using of a service to make a threat.

Section 17 criminalizes and sanctions the using of a service to make a hoax threat.

Section 18 criminalizes and sanctions the using of a service to menace, harass or cause harm. This section also makes reference to the terms "intimate visual recording" and "post an electronic communication" and its interpretation in this section. This can include revenge pornography.

PART 4 PROCEDURAL POWER

The purpose of these provisions for this Part of the Bill is to ensure that the obtaining and collecting of electronic evidence is done according to powers and procedures set out in this part. It also includes privacy safeguards and police accountability when carrying out their duties. This implements Article 14 to Article 21 under the Convention.

DIVISION 4.1 POWERS RELATING TO SEARCH WARRANTS ETC

Section 19 allows for an authorised officer to apply for a search warrant to a Supreme Court Judge. The Supreme Court Judge has the discretion to request for additional information when considering a request made under this section.

Section 20 allows for an authorised officer to make an urgent application, in limited circumstances, for a search warrant to a Supreme Court Judge.

Section 21 allows a Magistrate, appointed by the Lord Chief Justice, to deal with applications under this Division if a Supreme Court Judge is not available.

Section 22 provides for what a Supreme Court Judge shall consider when deciding whether or not to issue a search warrant.

Section 23 provides for what a Supreme Court Judge shall do once issuing an urgent search warrant applied for under section 20.

Section 24 provides for the contents of a search warrant.

Section 25 provides for the procedures to extend the duration of a search warrant.

Section 26 provides for the powers of an authorised officer when executing a search warrant.

Section 27 provides for the power of an authorised officer or a person assisting an authorised officer to access data on a seized computer system.

Section 28 provides for the powers and procedures of an authorised officer in securing etc. computer system or data storage medium under a search warrant.

Section 29 allows an authorised officer to direct a person searched, or a person in possession or control of, or has knowledge of the seized item to give reasonable assistance to the authorised officer. This section further sanctions a person who does not comply with the authorised officer's direction.

Section 30 provides an obligation to an authorised officer who is executing a power in a search warrant under section 26(1)(b) or section 29 of the Bill, to not cause damage to a computer system or data storage medium or data. This section also applies to any other person assisting the authorised officer.

Section 31 obliges an authorised officer to provide as soon as practicable, a receipt of whatever item that had been seized in the execution of a search warrant to the person searched, occupier of the place searched or if the place searched is not occupied then to leave the receipt in a conspicuous place at the place searched.

Section 32 provides for when a computer system or data storage medium should be returned and to whom it must be returned when it is no longer required. This section also provides for when a computer system or data storage medium should not be returned to a person or a place as this could possibly compromise investigation or prosecution of an offence.

Section 33 provides that an authorised officer takes reasonably necessary steps to minimise the need to retain the computer system or data storage medium.

Section 34 provides that an authorised officer who retains a computer system or data storage medium shall exercise reasonable care to prevent any damage. This section also applies to a person assisting the authorised officer.

Section 35 obliges the Police Commissioner to destroy data collected under a search warrant or any reproduction of that data under the control of Tonga Police when it is no longer useful for the investigation or prosecution of an offence.

Section 36 allows an authorised officer to make a written request to a person in control of a computer system for the preservation of data held in a computer system. This data can be preserved for a period of up to 90 days. This period can be further extended more than once for a period of not more than 90 days.

Section 37 allows an authorised officer to make an application to a Supreme Court Judge for the production of specified data held in a computer system. This includes a printout or other information that is reasonably required for the purpose of an investigation or proceeding.

Section 38 allows an authorised officer to use, make available for use or disclose things seized under a search warrant only for the purpose of preventing, investigating or prosecuting an offence. This may also be provided for at the request of a foreign law enforcement agency in accordance with this Division of the Bill and the Mutual Assistance in Criminal Matters Act.

Section 39 criminalises and sanctions any person who intends to hinder or obstruct an authorised officer or a person assisting, from conducting a search of a person or a place.

Division 4.2 specific provisions applying to service providers

Service Providers in providing their services to customers collect and store subscriber data, traffic data and content data. This Division of the Bill states the obligation of the Service Providers to comply with requests made to them in respect of the different types of data. Subdivisions 4.2.1, 4.2.2, 4.2.3 and 4.2.4 covers the disclosure of subscriber data, access to and disclosure of traffic data, preservation orders and interception warrants. To ensure that the data obtained from service providers are not misused or used in any other way other than for the purpose it was obtained, this Division provides a safeguard which obliges law enforcement to destroy this data that is in their control.

Subdivision 4.2.1 Disclosure of subscriber data

"Subscriber data" as defined in section 2 of the Bill means any data not including traffic or content data, held by a service provider (whether in the form of a computer data or any other form) in relation to a person using its services. This may include the subscriber's name, address or phone number.

Section 40 allows an authorized officer to make a written request to a service provider for the disclosure of subscriber data. A service provider is obliged to comply with the request as soon as practicable once it is received by them. Further terms of assistance between a service provider and Government can be established through a Memorandum of Understanding.

Section 41 is a safeguard provision in that it ensures that that subscriber data disclosed from a service provider under section 40 is only used for purposes stated in section 41 (1) sub-sections (a) to (f). This section also ensures that any data or any reproduction of this data, that is no longer needed for the purpose it was obtained is destroyed.

Subdivision 4.2.2 Access to and disclosure of traffic data

'Traffic data' as defined under section 2 of the Bill means:

(a) any computer data relating to an electronic communication that forms part of the chain of the communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

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

(c) any additional information relevant to the communication.

Traffic data can include the type of equipment that was used to relay the communication, the communication's origin, destination, route, time, size, duration or type or underlying service.

Section 42 allows an authorized officer to make a written request to a service provider for the disclosure of traffic data. A service provider is obliged to comply with the request as soon as practicable once it receives the request.

Section 43 allows the Police Commissioner or a Deputy Police Commissioner authorized by the Police Commissioner, to make a written request to a service provider for access to traffic data in real-time. The request can only be made for the enforcement of an offence punishable, on conviction, by imprisonment for at least 3 years.

Section 44 provides for when a request to access traffic data in real time comes into force and ceases to be in force. This section also states that the duration of the request can be for a period of up to 45 days from the day the request comes into force. Should law enforcement require more time, a new request will have to be made.

Section 45 provides for when the revocation notice of a request to access traffic data in real time is in force. The revocation must be made in writing to a service provider by the Police Commissioner or a Deputy Police Commissioner authorized by the Police Commissioner. The revocation notice must be served to the service provider as soon as practicable for their action.

Section 46 is a safeguard provision that ensures that the traffic data that is obtained under this Division of the Bill is only used for purposes set out in section 46(1) subsections (a) to (f). This section also ensures that any data or any reproduction of this data, that is no longer needed for the purpose it was obtained is destroyed.

Subdivision 4.2.3 preservation orders

Preservation Orders in this subdivision refers to stored computer data that has already been collected and retained by service providers. To preserve computer data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. This is important in computer or computer related investigations where computer data can be easily manipulated or changed through different ways. Also service providers may have their own policies on data retention and therefore it is vital that preservation of data prevents service providers from destroying data.

'Content data' as defined in section 2 of the Bill means data that forms the content or substance of a communication. This may include a short message service (SMS), an email or a post on social media.

Section 47 allows an authorized officer to issue a service provider with a preservation order for traffic and content data. This section also obliges the service provider to assist law enforcement further by disclosing a sufficient amount of traffic data so that other service providers involved in the communication transmission can be identified.

Section 48 provides for when the preservation order obtained under section 47(1) comes into force and its duration. The duration of a preservation order can be for a period of up to 90 days. This period can be extended more than once for a further period of up to 90 days by law enforcement. As investigations could possibly take longer than expected, this provision is to ensure that the integrity of the computer data being preserved is not compromised.

Section 49 provides for when the revocation notice for a preservation order is in force. The revocation must be made in writing to a service provider by an authorized officer before the order ceases to be in force or when it is no longer required. The authorized officer is obliged to inform the service provider about the revocation notice and give them a copy as soon as practicable.

SUBDIVISION 4.2.4 INTERCEPTION WARRANTS

Many computer or computer related crimes involve the transmitting of large quantities of data to one another through a computer system, which includes written text, visual images and sound. Some of this data being transmitted could be illegal content (e.g., child abuse material). Therefore, it is important that service providers and law enforcement have the capability to intercept these criminal intended communications. It is important to note that service providers would undertake interception on behalf of law enforcement.

Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization.

Sub- Division 4.2.4 interception warrants

Section 50 provides for when an authorised officer may make a sworn application to the Supreme Court for a warrant to intercept one or more services to allow access to and disclosure of content data, relating to a person believed to have used or is using a service.

Section 51 provides for when an authorised officer may make an unsworn application for an urgent, in limited circumstances, interception warrant to the Supreme Court. This section allows the application to be made by electronic means.

Section 52 provides for what the Supreme Court should consider independently, when assessing an application for an interception warrant made under section 50 or section 51.

Section 53 provides for the form and what it should contain in relation to an interception warrant issued under section 52. This must be prescribed by regulation.

Section 54 provides that the Supreme Court is to issue a copy of an interception warrant applied for under section 51 as soon as practicable to the authorised officer. This section also provides for what is to be done when the Supreme Court cannot provide a copy of the interception warrant to an authorised officer when reasonably practicable.

Section 55 provides for when an authorised officer is to serve the issued interception warrant to the service provider. This section also obliges the service provider to comply with the requirements of the interception warrant. The law enforcement need the assistance of the service provider in executing an interception warrant.

Section 56 provides for the lawful purposes for which content data disclosed under an interception warrant served under section 55 can be used. This section also ensures that any data or any reproduction of this data, that is no longer needed for the purpose it was obtained is destroyed.

Section 57 provides for the application by an authorised officer to the Supreme Court for the revocation of an interception warrant. The authorized officer is obliged to inform the service provider's authorised representative immediately about the revocation notice and give them a copy as soon as practicable. This is used only in circumstances where the police wish to revoke a warrant within the time limit for which it was used.

DIVISION 4.3 ASSISTANCE TO FOREIGN STATES

As computer crimes or computer enabled crimes are borderless it is vital that an effective and efficient mechanism for international co-operation is in place. The commission of these crimes mostly involves more than one State and therefore co-operation amongst these States must include a rapid flow of information and evidence. This Division of the Bill implements Tonga's obligation for international co-operation under the Convention.

Section 58 provides for a request by a foreign State to the Attorney General to arrange a service provider to preserve content or traffic data.

Section 59 provides for what the Attorney General shall consider when assessing a request by a foreign State for a foreign preservation order made under section 58 for the preservation of content or traffic data.

Section 60 provides for when a foreign preservation order comes into force and its duration. The duration of a foreign preservation order can be a period of up to 90 days. This period can be extended more than once for a further period of up to 90 days by the Attorney General.

Section 61 provides that traffic or content data preserved under a foreign preservation order may only be disclosed in accordance with section 70 and the Mutual Assistance in Criminal Matters Act.

Section 62 provides for the power of the Attorney General to revoke a foreign preservation order after it is made in relation to a foreign State. The Attorney General is obliged to inform the service provider's authorised representative immediately about the revocation notice and give them a copy as soon as practicable.

Section 63 provides for a request by the Attorney General to a service provider for disclosure of traffic data after receiving and considering a request made under section 4(2) of the Mutual Assistance in Criminal Matters Act from a foreign State. This section also obliges the service provider to comply with the request as soon as practicable after it is made. This section does not apply to traffic data in real time.

Section 64 provides for a request by the Attorney General to a service provider for disclosure of traffic data in real time after receiving and considering a request made under section 4(2) of the Mutual Assistance in Criminal Matters Act from a foreign State. This section also obliges the service provider to comply with the request as soon as practicable after it is made.

Section 65 provides for when a request made under section 64 to access traffic data in real time comes into force and its duration. The duration of the request can be a period of up to 21 days. This period can be extended only once for a further period of up to 21 days by the Attorney General.

Section 66 provides for the power of the Attorney General to revoke a request for access to traffic data in real time, under section 64. The Attorney General is obliged to inform the service provider's authorised representative about the revocation and give them a copy of the revocation immediately after the request is revoked.

Section 67 allows the Attorney General to make an application for a foreign interception warrant for the disclosure of either stored content data or preserved content data under a foreign preservation order or both, after a request is made under section 4(2) of the Mutual Assistance in Criminal Matters Act by a foreign State.

Section 68 provides for an application by the Attorney General to the Supreme Court for a foreign interception warrant requiring a service provider to allow access to and disclosure of content data for a request made under section 4(2) of the Mutual Assistance in Criminal Matters Act by a foreign State.

Section 69 provides for what the Supreme Court should consider when assessing an application for a foreign interception warrant made under section 68.

Section 70 provides for when the Attorney General may disclose traffic data, traffic data in real time or content data under a foreign interception order after receiving a request made under section 4(2) of the Mutual Assistance in Criminal Matters Act from a foreign State.

DIVISION 4.4 EVIDENTIARY CERTIFICATES

Evidentiary certificates are intended to provide evidence to the Court on the technical and operational matters that are undertaken in accessing procedural powers under the Act, In the case of a service provider, to provide written evidence on matters and to be conclusive proof of the matters stated in the document. This is intended to protect the commercial nature of the information and to assist the court in accepting technical evidence of the service provider. The service provider may be called to give additional evidence on matters not within the certificate.

The Police Commissioner or Deputy Police Commissioner authorised by the Police Commissioner may provide an evidentiary certificate to detail the technical and operation matters undertaken in relation to a request, order or warrant. A police evidentiary certificate is prima facie proof of the matters stated in the document. The police may be called to give evidence in relation to the certificate.

Section 71 provides for the issuing of an evidentiary certificate by an authorised representative of a service provider. This section also provides that an evidentiary certificate is to be accepted as evidence in proceedings without further proof and is conclusive evidence of matters stated in it.

Section 72 provides for the issuing of an evidentiary certificate by the Police Commissioner or Deputy Police Commissioner authorised by the Police Commissioner. This section also provides that an evidentiary certificate is to be accepted as evidence in proceedings without further proof and is conclusive evidence of matters stated in it.

DIVISION 4.5 OBLIGATIONS OF SERVICE PROVIDERS

Service providers enable subscribers to connect with others both domestically and internationally through the services they provide. It is therefore important that they co-operate and comply with the prevention, investigation and prosecution of computer crimes or computer enabled crimes.

Section 73 provides for the obligations placed on service providers. A service provider must do everything in their power to prevent their services from being used to commit a crime. A service provider is also obliged to provide reasonably necessary assistance to law enforcement.

Section 74 provides for terms and conditions in which service providers are to give assistance to Tonga Police. This section also provides the basis of which assistance must be given and it also states that a service provider may not profit nor lose from providing assistance to law enforcement.

PART 5 MISCELLANEOUS

Section 75 provides that an authorised officer may seek assistance from another person in exercising his power under this Bill.

Section 76 provides for the making of regulations by the Minister responsible, for the proper and efficient administration of this Bill.

Section 77 provides that the making or regulations by the Minister responsible, for transitional arrangements.

Section 78 provides the repealing of the Computer Crimes Act.

Hon. Poasi Tei
Minister of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change