Tonga

COMPUTER CRIMES ACT

Act 14 of 2003

COMPUTER CRIMES ACT

Arrangement of Sections

Section

PART I - PRELIMINARY **5**

1 Short Title 5
2 Interpretation 5
3 Jurisdiction 7

PART II - OFFENCES **7**

4 Illegal access 7
5 Interfering with data 8
6 Interfering with computer system 8
7 Illegal interception of data 8
8 Illegal devices 9

PART III - PROCEDURAL POWERS **9**

9 Search and seizure warrants 9
10 Assisting police 10
11 Production of data 11
12 Disclosure of traffic data 11
13 Preservation of data 11
14 Interception of electronic communications 12
15 Interception of traffic data 12
16 Evidence 12
17 Confidentiality and limitation of liability 12
18 Regulations 13

COMPUTER CRIMES ACT

Act 14 of 2003

AN ACT TO COMBAT COMPUTER CRIME AND TO PROVIDE FOR THE COLLECTION AND USE OF ELECTRONIC EVIDENCE

I assent,
TAUFA'AHAU TUPOU IV,
18th November, 2003

[8th September, 2003]

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

PART I - PRELIMINARY

1 Short Title

This Act may be cited as the Computer Crimes Act, 2003.

2 Interpretation

In this Act, unless the context otherwise requires:

"**computer**" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related

devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include;

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator; or

(c) a similar device which is non-programmable or which does not contain any data storage facility;

(d) such other device as the Minister may, by notification in the Gazette, prescribe;

"**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 data storage medium**" means any article or material such as a disk, from which information is capable of being reproduced, with or without the aid of any other article or device;

"**computer system**" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

"**hinder**", in relation to a computer system, means:

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

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system by any means; and

(d) inputting, deleting or altering computer data;

"**seize**" includes:

(a) make and retain a copy of computer data, including using on site equipment;

(b) render inaccessible, or remove, a computer, computer data in the accessed computer system; and

(c) take a printout of computer data;

"**service provider**" means a public or private entity that provides to users of its services the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of that entity or those users; and

"**traffic data**" means computer data that relates to a communication by means of a computer system; and is generated by a computer system that is part of the chain of communication, and shows the communication's

origin, destination, route, time, date, size, duration or the type of underlying services.

3 Jurisdiction

(1) Where an offence under this Act is committed by any person who is outside the Kingdom, he shall be deemed to have committed the offence within the Kingdom.

(2) For the purposes of this section, this Act shall apply as if, for the offence in question;

(a) the accused; or

(b) the computer, program or data.

was in the Kingdom at the material time.

PART II - OFFENCES

4 Illegal access

(1) For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

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

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including system related to essential emergency services.

(2) A person who wilfully, without lawful excuse, accesses any computer system commits an offence and shall be liable upon conviction to, a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both.

(3) A person who wilfully, without lawful excuse, accesses any protected computer commits an offence and shall be liable upon conviction to a fine not exceeding $100,000 or to imprisonment for a period not exceeding 20 years or to both.

(4) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in this section if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data is an offence.

5 Interfering with data

A person who, wilfully or recklessly without lawful excuse:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

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

(d) obstructs, interrupts or interferes with any person in the lawful use of data; or

(e) denies access to data to any person entitled to it;

commits an offence and shall be liable upon conviction, to a fine not exceeding $10,000 or to imprisonment for a period not exceeding 2 years or to both.

6 Interfering with computer system

A person who wilfully or recklessly, without lawful excuse:

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system,

commits an offence and shall be liable upon conviction to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.

7 Illegal interception of data

A person who, wilfully without lawful excuse, intercepts by technical means:

(a) any transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system that are carrying computer data,

commits an offence and shall be liable upon conviction, to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.

8 Illegal devices

(1) A person who:

(a) wilfully or recklessly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; or

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

with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; or

(b) has an item mentioned in subparagraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act;

commits an offence and shall be liable upon conviction to a fine not exceeding $20,000 or imprisonment for a period not exceeding 4 years or to both.

(2) A person who possesses more than one item mentioned in subsection (1) subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act.

PART III - PROCEDURAL POWERS

9 Search and seizure warrants

(1) If a magistrate is satisfied on sworn evidence that there are reasonable grounds to suspect that there may be in a place a computer, computer system, computer data or data storage medium which:

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

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

the magistrate may issue a warrant authorizing any police officer, with such assistance as may be necessary, to enter the place to search and seize the computer, computer system, computer data or data storage medium.

(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable:

(a) make a list of what has been seized, with the date and time of seizure; and

(b) give a copy of that list to —

(i) the occupier of the premises; or

(ii) the person in control of the computer system.

(3) Subject to subsection (4), on request, any police officer or another authorized person shall:

(a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or

(b) give the person a copy of the computer data.

(4) The police officer or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies may —

(a) constitute a criminal offence; or

(b) prejudice:

(i) the investigation in connection with which the search was carried out;

(ii) another ongoing investigation; or

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

10 Assisting police

(1) A person who is in possession or control of a computer, computer system, computer data or data storage medium that is the subject of a search under section 9 shall permit, and assist if required, the person making the search to —

(a) access and use a computer system or computer data storage medium to search any computer data available to or in the system;

(b) obtain and copy that computer data;

(c) use equipment to make copies; and

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

(2) A person who fails without lawful excuse to permit or assist a person acting under a search warrant commits an offence and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both.

11 Production of data

A magistrate on application by any police officer that specified computer data, or a printout or other information; is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order;

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

(b) an internet service provider to produce information about persons who subscribe to or otherwise use the service; and

(c) a person who has access to a specified computer system process to compile specified computer data from the system and give it to a specified person.

12 Disclosure of traffic data

Where a magistrate is satisfied on the basis of an application by any police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

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

13 Preservation of data

(1) Where any police officer is satisfied that:

(a) data stored in a computer system is reasonably required for the purpose of a criminal investigation; and

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

the police 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 be preserved for a period of up to 7 days as specified in the notice.

(2) The Magistrate may upon application authorize an extension not exceeding 14 days.

14 Interception of electronic communications

Where a magistrate is satisfied on the evidence that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate may:

(a) order an internet service provider to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

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

15 Interception of traffic data

(1) Where any police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to:

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

(b) permit and assist a specified police officer to collect or record that data.

(2) Where a magistrate is satisfied on the evidence that there are reasonable grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate may authorize any police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

16 Evidence

In proceedings for an offence under this Act the fact that:

(a) it is alleged that an offence of interfering with a computer system has been committed; and

(b) evidence has been generated from that computer system;

does not of itself prevent that evidence from being admitted.

17 Confidentiality and limitation of liability

(1) An Internet service provider who without lawful authority discloses:

(a) the fact that an order under sections 11, 12, 13, 14 and 15 has been made;

(b) anything done under the order; or

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

commits an offence and shall be liable upon conviction to a fine not exceeding $50,000 or imprisonment for a period not exceeding 10 years or to both.

(2) An internet service provider shall not be liable under any law for the disclosure of any data or other information that he discloses under sections, 11, 12, 13, 14, or 15.

18 Regulations

The Minister responsible for Communications may, with the consent of Cabinet make Regulations for the proper and efficient administration of this Act.

Passed in the Legislative Assembly this 8 day of September, 2003.