CYBERCRIME BILL 2020
(BILL NO. OF 2020)

CLAUSES

PART 1—PRELIMINARY

PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS

PART 3—COMPUTER-RELATED AND CONTENT-RELATED OFFENCES

PART 4—OTHER OFFENCES

PART 5—PROCEDURAL MEASURES

PART 6—INTERNATIONAL COOPERATION

A BILL

FOR AN ACT TO ADDRESS CYBERCRIME BY PROVIDING FOR THE GATHERING OF ELECTRONIC EVIDENCE AND THE REMEDIES IN RELATION TO CYBERCRIME AND FOR RELATED MATTERS

ENACTED by the Parliament of the Republic of Fiji—

PART 1—PRELIMINARY

Short title and commencement

1.—(1) This Act may be cited as the Cybercrime Act 2020.

(2) This Act comes into force on a date or dates appointed by the Minister by notice in the Gazette.

Interpretation

2. In this Act, unless the context otherwise requires—

"computer data" or "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 or a series of functions;

"computer program" or "program" means any computer data representing algorithms, codes, instructions or statements suitable to cause a computer system to perform a function or a series of functions;

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

"disciplined force" means—

(a) the Republic of Fiji Military Forces;
(b) the Fiji Police Force; or
(c) the Fiji Corrections Service;

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

(a) cut the electricity supply to a computer system;
(b) cause electromagnetic interference with a computer system;
(c) corrupt a computer system; or
(d) damage, delete, deteriorate, alter, modify or suppress computer data;

"hosting provider" means any person providing a computer data transmission service by storing information provided by a user of the service;

"information" means texts, messages, data, voice recordings, sounds, databases, videos, signals, software, computer programs, codes including object codes and source codes;

"Minister" means the Minister responsible for communications;

"service provider" means—

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or
(b) any other entity that processes or stores computer data on behalf of the entity or users of such service provided by the entity; and

"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication, or type of underlying service.

Application

3.—(1) Nothing in this Act affects the validity of any proceedings taken in relation to any offence under any other written law.

(2) This Act applies—

(a) where a person commits an offence under this Act while being present in Fiji;
(b) on board a ship flying the flag of Fiji;
(c) on board an aircraft registered under the laws of Fiji;
(d) where the alleged conduct was committed by a Fijian citizen, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State;
(e) where the computer, computer system, device, computer data or information affected or which was to be affected, by the act which constituted an offence under this Act, was at the material time lawfully accessible in Fiji;
(f) where the service, including any computer storage, or device or computer data or information processing service, used in the commission of an offence under this Act was accessible in Fiji; and
(g) where the loss or damage is caused in Fiji by the commission of an offence under this Act, to the State or to a person in Fiji.

(3) The provisions of this Act also apply to an offender present in Fiji when extradition of the person is not possible, solely on the basis of the person's nationality.

Savings of certain laws

4.—(1) Unless otherwise provided in this Act or any other written law, nothing in this Act affects—

(a) the liability, trial or punishment of a person for an offence under any other written law;

(b) the liability of a person to be tried or punished for an offence under any other written law relating to the jurisdiction of any court in respect of acts done beyond the ordinary jurisdiction of the court;
(c) the power of any court to punish a person for contempt of the court;
(d) the liability or trial of a person, or the punishment of a person under any sentence passed or to be passed, in respect of any act done or commenced before the commencement of this Act;
(e) any lawful power to grant any pardon or to remit or commute in whole or in part or to respite the execution of any sentence passed or to be passed; or
(f) any written law for a disciplined force.

(2) If a person performs an act which is punishable both under this Act and any other written law, the person may only be punished under only one such written law.

PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS

Unauthorised access to computer systems

5.—(1) Subject to subsection (5), a person who intentionally and without lawful authority or reasonable excuse causes a computer system to perform a function to secure access and knows that the access the person intends to secure is unauthorised, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

(2) A person secures access to a computer system if the person instructs, communicates with, stores data on, retrieves data from, or otherwise makes use of any resource of, the computer system.

(3) A person's access to a computer system is unauthorised if the person—

(a) is not entitled to control access of the kind in question; or
(b) does not have the consent of any person who is so entitled to have access of the kind in question.

(4) It is immaterial that the unauthorised access is not directed at—

(a) any particular computer data; or
(b) computer data held in any particular computer system.

(5) It is a defence if the person under subsection (1) if the person is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing.

Unauthorised interception of computer data or computer systems

6.—(1) Subject to subsection (5), a person who intentionally and without lawful authority or reasonable excuse intercepts or causes to be intercepted, directly or indirectly, any computer data or computer system, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

(2) In this section, an act of interception of any computer data to, from or within a computer system, includes listening to, recording or acquiring the substance, meaning or purpose of the computer data.

(3) It is immaterial that the unauthorised interception is not directed at—

(a) any particular computer data; or
(b) computer data held in any particular computer system.

(4) It is a defence if the person under subsection (1)—

(a) has the express consent of the person who sent the computer data and the intended recipient of the computer data; or
(b) is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing.

Unauthorised acts in relation to computer data or computer systems

7.—(1) A person commits an offence if—

(a) the person performs any unauthorised act in relation to a computer system or computer data;
(b) the person knows that the act is unauthorised when performing the act; and
(c) either subsection (3) or (4) applies.

(2) For the purpose of this section, there is an illegal data interference when a person who, intentionally and without lawful authority or reasonable excuse interferes with computer data owned or managed by another person by damage to, deletion, deterioration, alteration or suppression of, the computer data.

(3) This subsection applies if the person intends to—

(a) impair the operation of any computer system;
(b) prevent or hinder access to any computer data held in any computer system; or
(c) impair the operation or the reliability of any such computer data.

(4) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in subsection (2).

(5) The intention referred to in subsection (3) or the recklessness referred to in subsection (4) need not relate to—

(a) any particular computer system; or
(b) any particular computer data of any particular kind.

(6) An act performed in relation to a computer system is unauthorised if the person performing the act (or causing it to be done)—

(a) does not have responsibility for the computer system or computer data;
(b) is entitled to determine whether the act may be performed; and
(c) does not have prior written consent to the act from any such person.

(7) A person who commits an offence under subsection (1) is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

(8) In this section—

(a) a reference to performing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts; and
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

Unlawful supply or possession of computer system or other device, or computer data

8.—(1) A person who intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available a computer system or any other device, or computer data or computer program designed or adapted primarily for the purpose of committing an offence under this Part, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

(2) A person who is in possession of any computer data or computer program, or a computer system or any other device designed or adapted primarily for the purpose of committing an offence under this Part with the intention that it be used by the person or another person to commit or facilitate the commission of an offence under this Part, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 7 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

(3) For the purpose of subsection (2), possession of any computer data includes—

(a) possession of a computer system or computer data storage device that holds or contains the computer data;
(b) possession of a document in which the computer data is recorded; or
(c) having control of computer data that is in the possession of another person.

PART 3—COMPUTER-RELATED AND CONTENT-RELATED OFFENCES

Computer-related forgery

9. A person who without lawful authority or reasonable excuse inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intention of obtaining a gain for the person or another person, or causing loss to another person or exposing another person to risk of loss, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

Computer-related extortion and fraud

10. A person who intentionally without lawful authority or reasonable excuse performs or threatens to perform any act described under this Part for the purpose of procuring an economic benefit, for himself or herself or another person, or causing loss to another person or exposing another person to risk of loss, including by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of those acts, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

Child pornography

11. —(1) A person who intentionally—

(a) takes or permits to be taken child pornography;
(b) offers, distributes, makes available or shows child pornography;
(c) procures through a computer system and has in his or her possession child pornography for himself or herself or with a view of the content being distributed or shown to any other person; or
(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes such content or intends to do so,

commits an offence.

(2) In this section, "child pornography" means content that depicts, presents or represents––

(a) a child engaged in sexual intercourse or sexually explicit conduct;
(b) a person appearing to be a child in sexual intercourse or sexually explicit conduct; or
(c) an image, animation, text material or video of a child engaged in sexual intercourse or sexually explicit conduct that includes any audio, visual or text material.

(3) Where—

(a) the impression conveyed by the content is that the person shown is a child; or
(b) the predominant impression conveyed is that the person shown is a child, notwithstanding that the person's physical characteristics are those of an adult,

the content must be treated for all purposes of this section as showing a child.

(4) A person who commits an offence under this section is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 15 years or both; and
(b) in the case of a body corporate, a fine not exceeding $200,000.

(5) The court before which a person is convicted of an offence under this section may, in addition to any penalty imposed, order—

(a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; or
(b) that the material subject matter of the offence no longer be stored on and be made available through the computer system, or that the material be deleted.

PART 4—OTHER OFFENCES

Identity theft

12. Any person who without lawful authority or reasonable excuse intentionally transfers, possesses or uses through or by a computer system the identification or means of identification of another person with intent to commit or to aid or abet, or in connection with any unlawful activity that constitutes a crime, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

Theft of telecommunication services

13. A person who without lawful authority or reasonable excuse uses a computer and intentionally transfers, possesses or uses the telecommunication services of another person with the intent to commit or to aid and abet, or in connection with any unlawful activity that constitutes a crime, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

Disclosure during an investigation

14. Any person who without lawful authority or reasonable excuse discloses during an investigation—

(a) the fact that an order that confidentiality is to be maintained, has been made;
(b) anything done under such an order; or
(c) any data collected or recorded under the order,

commits an offence and is liable on conviction to—

(i) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(ii) in the case of a body corporate, a fine not exceeding $50,000.

Failure to provide assistance

15. A person, other than a suspect who, without lawful authority or reasonable excuse fails to provide assistance or assist a person presenting an order under this Act, commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $5000 or imprisonment for a term not exceeding 2 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

PART 5—PROCEDURAL MEASURES

General procedural powers

16. All powers and procedures under this Act are applicable to and may be exercised with respect to any—

(a) criminal offence established in accordance with this Act;
(b) other criminal offences committed by means of a computer system established under any other written law; and
(c) the collection of evidence in electronic form of a criminal offence under this Act or any other written law.

Search and seizure

17. —(1) A police officer or authorised person may apply to a judge or magistrate for a warrant to enter a particular location to search and seize a computer, computer program, computer system, device or computer data, including search or obtain similar access to—

(a) a computer system or part thereof and computer data stored therein; and
(b) a computer storage medium in which computer data may be stored in the territory of the country.

(2) The judge or magistrate may issue the warrant, with or without the assistance of an expert, if the judge or magistrate is satisfied on the basis of sworn evidence, affidavit, information that there are reasonable grounds to suspect or believe that the computer program, computer system, device or computer data in the particular location—

(a) may be material as evidence in proving an offence; or
(b) has been acquired by a person as a result of an offence.

(3) For the purposes of this Part and notwithstanding section 15 of the Criminal Procedure Act 2009, "to seize" includes to—

(a) activate any onsite computer system and electronic storage media;
(b) make and retain a copy of computer data, including by using on-site equipment;
(c) maintain the integrity of the relevant stored computer data;
(d) render inaccessible or removing computer data in the accessed electronic system;
(e) take a printout of output of computer data; or
(f) secure a computer system or part of it or an electronic storage medium.

(4) A police officer or other authorised person who conducts a search and seizes material or evidence under this section must, 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 such computer, computer program, computer system, device or computer data.

(5) Subject to subsection (6), a police officer or other authorised person must, on request––

(a) permit a person who had custody or control of the computer, computer program, computer system, device or computer data, or someone acting on their behalf to access and copy computer data on the system; or
(b) gives the person a copy of the computer data obtained pursuant to an order under subsection (1).

(6) The police officer or other authorised person may refuse to give access or provide copies if he or she has reasonable grounds to believe that providing access or copies may—

(a) constitute an offence under the Crimes Act 2009;
(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.

(7) A police officer or other authorised person who is undertaking a search is empowered to seize or similarly secure computer data accessed in accordance with subsections (1) and (2).

Admissibility of evidence

18. —(1) In any proceedings related to any offence under any written law, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a computer system must not of itself prevent that evidence from being presented, relied on or admitted.

(2) The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under any written law, when exercised lawfully by a police officer or other authorised person, or any regulatory authority that by itself does not investigate or prosecute an offence.

Expedited preservation of stored computer data

19. —(1) A police officer or other authorised person may issue a written notice to a person to preserve specified computer data stored by means of a computer system if the police officer or other authorised person is satisfied that—

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

(b) there is a risk or vulnerability that the specified computer data may be modified, lost, destroyed or rendered inaccessible.

(2) The police officer or authorised person may serve the written notice on any person in possession or control of the computer, computer program, computer system, device or computer data, requiring the person to expeditiously preserve the specified computer data.

(3) The written notice must specify a maximum period of 90 days for which the specified computer data is to be preserved and maintained for integrity and may be renewed once, for a further maximum period of 90 days.

(4) A person who is served a written notice must keep the notice and all information about it confidential, unless expressly permitted by the police officer or authorised person.

(5) A person who contravenes this section commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

Expedited preservation and partial disclosure of traffic data

20. —(1) If a police officer or other authorised person is satisfied that—

(a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system in the possession of or controlled by a service provider is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk or vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible,

the police officer or other authorised person may, by written order given to the service provider in possession or control of the computer system or computer data storage medium, require the service provider to—

(i) undertake expeditious preservation and maintenance of integrity of the specified traffic data for a period specified in the notice not exceeding 90 days, regardless of whether one or more service providers were involved in the transmission of that communication; and
(ii) disclose sufficient traffic data about any communication to identify—

(A) the service provider; and
(B) the path through which the communication was transmitted.

(2) On application by the police officer or authorised person, the period of preservation and maintenance for integrity may be extended beyond 90 days if a judge authorises an extension for a further specified period of time, provided the judge is satisfied that—

(a) such extension of preservation is reasonably required for the purposes of a criminal investigation or prosecution;

(b) there is a risk or vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible; and
(c) the cost of such preservation is not overly burdensome on the person in possession or control of the computer system.

(3) A service provider who is served a notice must keep the notice and all information about it confidential, unless expressly permitted by the senior police officer or the judge granting authorisation under subsection (2).

(4) A service provider under subsection (3) must—

(a) respond expeditiously to requests for assistance; and
(b) disclose as soon as practicable, a sufficient amount of traffic data to enable a police officer or other authorised person to identify any other service provider involved in the transmission of the communication.

(5) The powers of the police officer or other authorised person under subsection (1) apply whether there is one or more service providers involved in the transmission of communication which is subject to the exercise of powers under this section.

(6) A service provider who contravenes this section commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both; and
(b) in the case of a body corporate, a fine not exceeding $100,000.

Production order

21. —(1) If on an application made under oath and affidavit, a police officer or other authorised person demonstrates to the satisfaction of a judge or magistrate that there exist reasonable grounds to believe that—

(a) specified computer data stored in a computer system or a computer data storage medium in the possession or control of a person in Fiji; or
(b) specified subscriber information relating to services offered in Fiji are in that service provider's possession or control which is necessary or desirable for the purposes of any investigation,

the judge may order—

(i) such person in Fiji to submit the specified computer data in that person's possession or control, which is stored in a computer system or a computer data storage medium; or
(ii) such a service provider offering its services in Fiji to submit subscriber information relating to such services in that service provider's possession or control.

(2) In this section, "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic data or content data and which can be established by—

(a) the type of communication service used and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

(3) The judge may also require that the recipient of the order and any person in control of the computer system keep confidential the existence of the warrant and exercise of power under this section.

(4) A person who contravenes an order granted under this section commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both; and
(b) in the case of a body corporate, a fine not exceeding $50,000.

(5) When making an application under subsection (1), the police officer or other authorised person must provide the following—

(a) reasons as to why the specified computer data sought is likely to be available with the persons mentioned in subsection (1);
(b) the investigation that may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;
(c) identify and explain with specificity the type of evidence suspected is likely to be produced by the persons mentioned in subsection (1);
(d) identify and explain with specificity the subscribers, users or unique identifiers which are the subject of an investigation or prosecution which are believed may be disclosed as a result of the production of the specified computer data;
(e) identify and explain with specificity the identified offence made out in respect of which the production order is sought;
(f) the measures that are to be taken to ensure that the specified computer data will be produced—

(i) whilst maintaining the privacy of other users, customers and third parties; and
(ii) without the disclosure of data of any party which is not part of the investigation; and

(g) the measures to be taken to prepare and ensure that the production of the specified computer data is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.

Search and seizure of stored computer data

22. —(1) If upon an application made under oath and affidavit, a police officer or other authorised person under this Act demonstrates to the satisfaction of a judge or magistrate that there exist reasonable grounds to believe that there may be in a specified computer system, program, data, or computer data storage medium that—

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence; or

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

the judge may issue a warrant authorising a police officer or other authorised person, with such assistance as may be necessary, to—

(i) seize or similarly secure the specified computer system, program, data or computer data storage medium;

(ii) inspect and check the operation of any computer system to which the warrant issued under this section applies;

(iii) require any person, other than the suspect, possessing knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary computer data or information, to enable the police officer or other authorised person in conducting such activities as authorised under this section;

(iv) require any person, other than the suspect, in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of the warrant issued under this section; or

(v) provide the police officer or other authorised person with such reasonable technical and other assistance as the police officer or other authorised person may require for the purposes of the warrant issued under this section.

(2) When making an application under subsection (1), the police officer or other authorised person must provide the following substantive grounds—

(a) reasons as to why the material sought will be found on the specified computer system, program, data or computer data storage medium to be searched;

(b) identify and specify the type of evidence suspected to be found on the premises; and

(c) the measures to be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer system, program, data, computer data storage medium.

(3) Where a police officer or other authorised person under this Act is permitted to search or similarly access a specified computer system, program, data, or computer data storage medium, under subsection (1), and has grounds to believe that the data sought is stored in another computer system, and such data is lawfully accessible from or available to the initial system, the police officer or other authorised person may extend the search or similar accessing to such other system or systems.

(4) Seized computer data may be used only for lawful purposes, being the purpose for which it was originally obtained, or to enforce the criminal law.

(5) The police officer or other authorised person must—

(a) only seize a computer system under subsection (1) when—

(i) it is not practical to seize or similarly secure the computer data; or
(ii) it is necessary to ensure that data will not be destroyed, altered or otherwise interfered with;

(b) exercise reasonable care while the computer system or computer data storage medium is retained.

(6) Any person who wilfully obstructs the lawful exercise of the powers under this section or misuses the powers granted under this section commits an offence and is liable on conviction to—

(a) in the case of an individual, a fine not exceeding $5000 or imprisonment for a term not exceeding 2 years or both; and
(b) in the case of a body corporate, a fine not exceeding $10,000.

(7) In this section—

"decryption information" means information or technology that enables a person to readily unscramble encrypted data into an intelligible format;

"encrypted data" means data which has been transformed from its plain text version to an unintelligible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; and

"unencrypted version" means original data before it has been transformed into an unintelligible format.

Real time collection of traffic data

23. —(1) Upon an application made under oath or affidavit, a police officer or other authorised person must demonstrate to the satisfaction of a judge or magistrate that there are reasonable grounds to believe that traffic data associated with specified communications and related to or connected with a person under investigation is reasonably required for the purposes of a specific criminal investigation, a judge may issue a warrant requiring a service provider, to—

(a) collect or record traffic data in real-time; and
(b) provide only the traffic data to the authorised person,

provided that such real-time collection or recording of traffic data must not be ordered for a period beyond that which is absolutely necessary and in any event for a period not exceeding 90 days.

(2) When issuing a warrant under subsection (1), the judge or magistrate must be satisfied that—

(a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(b) measures to be taken to ensure that the data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and
(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(3) The period of real-time collection or recording of traffic data may be extended beyond 90 days if, on an application, a judge authorises an extension for a further specified period of time, not exceeding a further period of 90 days.

(4) When making an application under subsection (1), the police officer or other authorised person under this Act must provide the following substantive grounds and reasons also—

(a) explain why it is believed the traffic data sought will be available with the person in control of the computer system;
(b) identify and explain with specificity the type of traffic data suspected will be found on such computer system;
(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system;
(d) identify and explain with specificity the identified offences in respect of which the warrant is sought;
(e) what measures are to be taken to prepare and ensure that the traffic data will be sought and carried out—

(i) whilst maintaining the privacy of other users, customers and third parties; and
(ii) without the disclosure of data of any party not part of the investigation.

(5) A judge may also require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(6) Where obligations have been imposed on a service provider under this Part, the steps which it are reasonably practicable for the service provider to take include every step which it would have been reasonably practicable for the service provider to take if it had complied with its obligations.

(7) A service provider who contravenes this section is liable on conviction to a fine not exceeding $100,000.

Interception of content data

24. —(1) If upon an application made under oath and affidavit, a police officer or other authorised person demonstrates to the satisfaction of a judge or magistrate that there are reasonable grounds to authorise the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes—

(a) investigation and prosecution of serious offences; or
(b) to give effect to a mutual assistance request,

a judge or magistrate may issue a warrant requiring a service provider, to—

(i) intercept the content data in real-time; and
(ii) provide that content data to the authorised person as soon as reasonably practicable,

provided that the real-time interception of content data is not to be ordered for a period beyond what is absolutely necessary and, in any event, not exceeding 90 days.

(2) When issuing a warrant under subsection (1), the judge or magistrate must be satisfied that—

(a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
(b) measures are to be taken to ensure that the content data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and content data of any party not part of the investigation; and
(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(3) When making an application under subsection (1), the police officer or other authorised person must provide the following—

(a) reasons as to why the content data sought will be available with the person in control of the computer system;
(b) identify and explain with specificity the type of content data suspected will be found on such computer system;
(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system;
(d) identify and explain with specificity the identified offences in respect of which the warrant is sought;
(e) the measures to be taken to prepare and ensure that the content data will be sought and carried out—

(i) whilst maintaining the privacy of other users, customers and third parties; and
(ii) without the disclosure of data of any party not part of the investigation.

(4) The period of real-time interception of content data may be extended beyond the 90-day period if, on an application, a judge authorises an extension for a further specified period of time, not exceeding a further period of 90 days.

(5) A judge must require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(6) The Minister may determine that a service provider must implement the capability to allow interception under this section, including specifying the technical requirements and standards for the capability.

(7) Where obligations have been imposed on a service provider under subsection (1), the steps which are reasonably practicable for the service provider to take include every step which would have been reasonably practicable for the service provider to take if it had complied with its obligations.

(8) A service provider who contravenes a warrant issued under this section commits an offence and is liable on conviction to a fine not exceeding $100,000.

PART 6—INTERNATIONAL COOPERATION

General principles relating to international cooperation

25. —(1) The Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the purposes of investigations or proceedings concerning offences related to computer systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act.

(2) Subject to the Mutual Assistance in Criminal Matters Act 1997, the Government may–
–

(a) make requests on behalf of Fiji to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Fiji, relating to any serious offence.

(b) in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence—

(i) grant the request, in whole or in part, on such terms and conditions as the Government thinks fit;

(ii) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty, security of Fiji or would otherwise be against the public interest;

(iii) after consulting with the appropriate authority of the foreign State, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Fiji; or

(iv) postpone action on a request if such action would prejudice an investigation or proceeding in Fiji.

Extradition

26. The offences under Parts 2 to 4 are considered extraditable offences under the Extradition Act 2003.

Spontaneous information

27. —(1) The Government may, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out

investigations or proceedings or might lead to a request for cooperation by the foreign State under this Act.

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

(3) If the foreign State is unable to comply with such conditions under subsection (2), the foreign government must notify the Government, which must then determine whether the information may be provided

Confidentiality and limitation on use

28. —(1) Where the Mutual Assistance in Criminal Matters Act 1997 is not applicable to a foreign State, the Government may require that foreign State to—

(a) keep confidential the contents of any information or material provided by the Government;
(b) only use the contents and any information and material provided by the Government for the purpose of a specified criminal investigation; and
(c) comply with any such other conditions of use as specified by the Government.

(2) A request made on behalf of Fiji to a foreign State for assistance under this provision must be made only by or with the authority of the Attorney-General.

Expedited preservation of stored computer data

29. —(1) Subject to any limitations specified in this Part, a foreign government, foreign agency or any international agency may request the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of data stored by means of a computer system, located within Fiji or control of the Government and in respect of which the requesting foreign government, foreign agency or international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

(2) A request for preservation made under subsection (1) must specify—

(a) the authority seeking the preservation;
(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
(c) the stored computer data to be preserved and its relationship to the offence;
(d) any available information identifying the custodian of the stored computer data or the location of the computer system;
(e) the necessity of the preservation; and
(f) that the foreign government, foreign agency or international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(3) Upon receiving the request under this subsection (1), the Attorney-General or 24/7 network must take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act.

(4) Any preservation effected in response to the request referred to under this section must be for a renewable period not less than 60 days, in order to enable the foreign government,

foreign agency or international agency to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request, the data must continue to be preserved until a final decision is taken on that request.

Expedited disclosure of preserved traffic data

30. Where during the course of executing a request under this Act with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Attorney-General or 24/7 network, must expeditiously disclose to the requesting foreign government, foreign agency or international agency a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

Mutual assistance regarding accessing of stored computer data

31. —(1) Subject to any limitations specified by the Government, a foreign government, foreign agency or international agency may request the investigation agency to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within Fiji, including data that has been preserved pursuant to section 29.

(2) A request for mutual assistance regarding accessing of stored computer data must as far as practicable—

(a) give the name of the authority conducting the investigation or proceeding to which the request relates;
(b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws;
(c) give a description of the purpose of the request and of the nature of the assistance being sought;
(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in Fiji, give details of the offence in question, particulars of any investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;
(e) give details of any procedure that the requesting State wishes to be followed by Fiji in giving effect to the request, particularly in the case of a request to take evidence;
(f) include a statement setting out any requirements of the requesting State concerning any confidentiality relating to the request and the reasons for those requirements;
(g) give details of the period within which the requesting State wishes the request to be complied with;
(h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in Fiji;
(i) give details of the stored computer data, data or program to be seized and its relationship to the offence;
(j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or electronic device;
(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and
(l) give any other information that may assist in giving effect to the request.

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

(4) Upon obtaining necessary authorisation including any warrants to execute the request, the investigation agency may seek the support and cooperation of the foreign government, foreign agency or international agency during the search and seizure.

(5) Upon conducting the search and seizure request the investigation agency must, subject to this section, provide the results of such search and seizure and the electronic or physical evidence so seized to the foreign government, foreign agency or the international agency.

Transborder access to stored computer data with consent or where publicly available

32. A police officer or other authorised person may, subject to any applicable provisions of this Act—

(a) access publicly available (open source) stored computer data, regardless of where the data is located; or
(b) access or receive, through a computer system in Fiji, stored computer data located in another territory of a state with whom Fiji has an applicable international agreement,

if such police officer or other authorised person obtains the lawful and voluntary consent of the person who has lawful authority to disclose the data through that computer system.

Mutual assistance regarding the real-time collection of traffic data

33. —(1) Subject to any limitations specified by the Government, a foreign government, foreign agency or any international agency may request the Attorney-General to provide assistance in real-time collection of traffic data associated with specified communications in Fiji transmitted by means of a computer system.

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

(a) the authority seeking the use of powers under this section;
(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
(c) the name of the authority with access to the relevant traffic data;
(d) the location at which the traffic data may be held;
(e) the intended purpose for the required traffic data;
(f) sufficient information to identify the traffic data;
(g) any further details relevant traffic data;
(h) the necessity for use of powers under this section; and
(i) the terms for the use and disclosure of the traffic data to third parties.

(3) Upon receiving the request under subsection (1), the Attorney-General must take all appropriate measures to obtain necessary authorisation including any warrants to execute the request in accordance with the procedures and powers provided under Part 5.

(4) Upon obtaining necessary authorisation including any warrants to execute the request, the Attorney-General may seek the support and cooperation of the foreign government, foreign agency or the international agency during the search and seizure.

(5) Upon conducting the measures under this section, the Attorney-General must provide the results of such measures and real-time collection of traffic data associated with specified communications to the foreign government, foreign agency or the international agency.

Mutual assistance regarding the interception of content data

34. —(1) Subject to any limitations specified by the Government, a foreign government, foreign agency or any international agency may request the Attorney-General to provide assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system in Fiji transmitted by means of a computer system.

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

(a) the authority seeking the use of powers under this section;
(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
(c) the name of the authority with access to the relevant communication;
(d) the location at which or nature of the communication;
(e) the intended purpose for the required communication;
(f) sufficient information to identify the communications;
(g) details of the data of the relevant interception;
(h) the recipient of the communication;
(i) the intended duration for the use of the communication;
(j) the necessity for use of powers under this section; and
(k) the terms for the use and disclosure of the communication to third parties.

(3) Upon receiving the request under subsection (1), the Attorney-General must, if the request is in relation to an offence punishable with at least 5 years of imprisonment, take all appropriate measures to obtain necessary authorisation including any warrants to execute on the request in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining necessary authorisation including any warrants to execute on the request, the Attorney-General may seek the support and cooperation of the foreign government, foreign agency or the international agency during the search and seizure.

(5) Upon conducting the measures under this section, the Attorney-General must provide the results of such measures and real-time collection or recording of content data of specified communications to the foreign government, foreign agency or the international agency.

24/7 Network

35. —(1) The Minister must designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, which assistance must include facilitating, or, if permitted by written law and practice of Fiji, directly carrying out the following measures—

(a) the provision of technical advice;
(b) the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data;

(c) the collection of evidence, the provision of legal information, and locating of suspects;
(d) within expeditious timelines to be defined by regulations.

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

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

PART 7—MISCELLANEOUS

Regulations

36. —(1) The Minister may make regulations to prescribe matters that are required or permitted by this Act to be prescribed or are necessary or convenient to be prescribed for carrying out or giving effect to this Act and generally for achieving the purposes of this Act.

(2) Without affecting the generality of subsection (1), the Minister may make regulations prescribing offences and penalties not exceeding—

(a) in the case of an individual, a 50,000 or imprisonment for a term of 15 years or both; or
(b) in the case of body corporate, a fine of $ 200,000.

Office of the Attorney-General
Suvavou House
Suva

February 2020

CYBERCRIME BILL 2020

EXPLANATORY NOTE

(This note is not part of the Bill and is intended only to indicate its general effect)

1.0 BACKGROUND

1.1 In 2016, the Fijian Government launched its Cyber security strategy which *inter alia* provided for cybercrime legislation to be developed in order to enable cyber issues and in particular cybercrime offences to be prosecuted in Fiji.

1.2 The International Convention on Cybercrime ('Budapest Convention') provides guidance on legislative requirements and in particular provides avenues for member States to have access to information as well as encourages information sharing on a wider platform that would greatly assist Fiji in this area.

1.3 The Cybercrime Bill 2019 (**'Bill'**) therefore seeks to align to the requirements under the Budapest Convention and introduces new provisions on substantive cybercrime offences, procedural requirements, remedies in relation to cybercrime offences, the collection of electronic evidence and international cooperation for this purpose.

1.4 The Bill introduces specific provisions on offences against the confidentiality, integrity and availability of computer data and computer systems such as unauthorised access to and unauthorised interception of, computer systems or computer data. Other computer-related and content-related offences included in the Bill are computer related forgery, computer related fraud and child pornography.

1.5 The Bill also enables the investigation and prosecution of such offences and introduces procedural measures for the collection of evidence in electronic form particularly for real time collection of data and expedited preservation of stored computer data.

2.0 CLAUSES

2.1 The Bill consists of 7 parts and 36 clauses.

2.2 Part 1 of the Bill provides the preliminary provisions.

2.3 Clause 1 of the Bill provides for the short title and commencement. If passed by Parliament, the new legislation will come into force on a date or dates appointed by the Minister by notice in the Gazette.

2.4 Clause 2 of the Bill provides for the definitions of the terms used in the Bill.

2.5 Clause 3 of the Bill provides for the application of the provisions. If passed by Parliament, the new legislation will apply to *inter alia* a person present in the territory of Fiji when extradition of the person is not possible, solely on the basis of the person's nationality.

2.6 Clause 4 of the Bill provides for the savings of certain laws. For instance, clause 4 of the Bill provides unless otherwise provided in the Bill or any other written law, nothing in the Bill affects *inter alia* the liability, trial or punishment of a person for an offence under any other written law. In addition, clause 4 provides that if a person performs an act which is punishable both under the Bill and any other written law, the person may only be punished under one such applicable written law.

2.7 Part 2 of the Bill provides for offences against the confidentiality, integrity and availability of computer data and computer systems.

2.8 Clause 5 of the Bill provides for the offence of unauthorised access to computer systems and the applicable penalties for individuals and body corporates. Clause 5 also outlines what "securing access to a computer system" means and the circumstances in which such access is unauthorised. In addition, clause 5 provides that in terms of the offence of unauthorised access to computer systems, it is a defence if a person is acting in reliance of any statutory power for the purpose of *inter alia* obtaining information.

2.9 Clause 6 of the Bill provides for the offence of unauthorised interception of computer data or computer systems and the applicable penalties for individuals and body corporates. Clause 6 also outlines what "an act of interception of any computer data to, from and within a computer system" means. In addition, clause 6 provides that in terms of the offence of unauthorised interception of computer data, it is a defence if a person has the express consent of the person who sent the computer data and the intended recipient of the computer data, or if a person is acting in reliance of an authorisation under a court order or any statutory power.

2.10 Clause 7 of the Bill provides for the offence of unauthorised acts in relation to a computer system or computer data and the applicable penalties for individuals and body corporates. Clause 7 also outlines what "illegal data interference" means and the circumstances in which an act performed in relation to a computer system is unauthorised.

2.11 Clause 8 of the Bill provides for the offence of unlawful supply or possession of a computer system or other device, or computer data and the applicable penalties for individuals and body corporates. Clause 8 also outlines what "possession of any computer data" means.

2.12 Part 3 of the Bill provides for computer-related and content-related offences.

2.13 Clause 9 of the Bill provides for the offence of computer-related forgery and the applicable penalties for individuals and body corporates.

2.14 Clause 10 of the Bill provides for the offence of computer-related extortion and fraud, and the applicable penalties for individuals and body corporates.

2.15 Clause 11 of the Bill provides for the offence of child pornography and the applicable penalties for individuals and body corporates. Clause 11 also outlines what "child pornography" means as well as provides the additional orders a court may make when convicting a person for the offence of child pornography.

2.16 Part 4 of the Bill provides for other offences such as identity and telecommunication services theft.

2.17 Clause 12 of the Bill provides for the offence of identity theft, specifically the unlawful use of a computer system to intentionally transfer, possess or use a means of identification of another person with the intent to commit or to aid or abet in an activity that constitutes an offence. Clause 12 also provides for the penalties for the offence of identity theft, as applicable to individuals and body corporates.

2.18 Clause 13 of the Bill provides for the offence of theft or telecommunication services, specifically the unlawful use of a computer system to intentionally transfer, possess or use the telecommunication services or another person with the intent to commit or to aid or abet in an activity that constitutes an offence. Clause 13 also provides for the penalties for the offence of theft of telecommunication services, as applicable to individuals and body corporates.

2.19 Clause 14 of the Bill provides for the offence of disclosure during an investigation, specifically the unlawful disclosure during an investigation of an order to maintain confidentiality, or anything done under such order, or any data collected or recorded under such order. Clause 14 also provides the penalties for the offence of disclosure during an investigation, as applicable to individuals and body corporates.

2.20 Clause 15 of the Bill provides for the offence of failure to provide assistance, specifically the unlawful failure by a person to provide assistance or to assist a person presenting an order. Clause 15 also provides the penalties for the offence of failure to provide assistance, as applicable to individuals and body corporates.

2.21 Part 5 of the Bill provides for procedural measures.

2.22 Clause 16 of the Bill provides for the general procedural powers, specifically that all powers and procedures under the Bill are applicable to and may be exercised with respect to *inter alia* any criminal offence established in accordance with the Bill and any other criminal offence committed by means of a computer system established under any other written law.

2.23 Clause 17 of the Bill provides for search and seizure powers. A police officer or an authorised person may apply to a judge or magistrate for a warrant to enter a particular location to search and seize *inter alia* a computer or computer program. In addition, clause 17 provides that a judge or magistrate may issue the warrant, with or without the assistance of an expert if he or she is satisfied on the evidence and information presented, that the sought computer program, computer system, device or computer data may be material as evidence in proving an offence or acquired as a result of an

offence. Clause 17 also outlines what "to seize" means for the purposes of Part 5 of the Bill. Furthermore, clause 17 provides for the creation of lists outlining all materials seized, the circumstances in which a police officer or authorised person must permit a person to access computer data which has been seized and the circumstances in which a police officer or authorised person may refuse such access.

2.24 Clause 18 of the Bill provides for the admissibility of evidence. Essentially, clause 18 provides that in terms of any proceedings related to any offence under any written law, the fact that evidence has been *inter alia* generated in a search of a computer system must not itself prevent that evidence from being presented, relied on or admitted. In addition, clause 18 provides that the powers and procedures provided under Part 5 of the Bill are without prejudice to the powers granted under any written law when exercised lawfully by a police officer.

2.25 Clause 19 of the Bill provides for the expedited preservation of stored computer data, specifically the circumstances in which a police officer or other authorised person may issue a written notice to a person to preserve computer data stored by means of a computer system. Clause 19 also provides that the notice must specify a timeframe of 90 days for which the specified computer data must be preserved and which may be renewed once, for a further period of 90 days. In addition, clause 19 provides the penalties applicable to individuals and body corporates when in breach of the requirements under clause 19.

2.26 Clause 20 of the Bill provides for expedited preservation and partial disclosure of traffic data. Essentially, clause 20 provides that a police officer or other authorised person may, by written order, require a service provider to preserve specified traffic data for a period of time in an expeditious manner, regardless of whether one or more service providers were involved in the transmission of the communication in question. Clause 20 also provides the applicable penalties for service providers should the service providers fail to comply with the requirements of clause 20.

2.27 Clause 21 of the Bill provides that a judge or magistrate may order a person in Fiji to submit specified computer data in that person's possession or control or a service provider offering its services in Fiji to submit subscriber information relating to such services in that service provider's possession or control, upon application made by a police officer or other authorised person. Clause 21 also provides that in order for a for an order to be made, the application must demonstrate to the satisfaction of the judge or magistrate that there are reasonable grounds that the specified computer data or subscriber information is in the possession or control of a person in Fiji or a service provider offering services in Fiji or are required or desirable for the purposes of an investigation. In addition, clause 21 also provides the applicable penalties for failure to comply with an order issued under clause 21.

2.28 Clause 22 of the Bill provides that a judge may issue a warrant authorising a police office or other authorised person, to *inter alia* search and seize stored computer data. Clause 22 also provides that in order for a judge or magistrate to issue the warrant, the application for the warrant must satisfy the judge or magistrate that there are reasonable grounds that there may be in a specified computer system, for instance, that is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence. In

addition, clause 22 provides the applicable penalties for wilfully obstructing or misusing the lawful powers provided therein. Clause 22 also provides for the definitions of "decrypted information", "encrypted data" and "unencrypted version", which are definitions specifically relevant to clause 22.

2.29 Clause 23 of the Bill provides that a judge or magistrate may issue a warrant requiring a service provider to collect or record traffic data in real-time and provide only the traffic data to an authorised officer. Clause 23 also provides that a judge or magistrate may only issue such a warrant if the application made provides to the satisfaction of the judge or magistrate reasonable grounds that the traffic data associated with specified communications and related to or connected with a person under investigation is reasonably required for a specific criminal investigation. In addition, clause 23 elaborates on the substantive grounds that must be provided in an application for such a warrant and, similarly to other provisions under the Bill, provides that a judge or magistrate may also require a service provider to keep the warrant issued confidential. Clause 23 also provides the penalty applicable to a service provider if the service provider contravenes clause 23.

2.30 Clause 24 of the Bill provides that a judge or magistrate may issue a warrant requiring a service provider to intercept content in real-time and provide that content to an authorised officer as soon as reasonably practicable. Clause 24 also provides that a judge or magistrate may only issue such a warrant if satisfied that the interception of content data is related to or connected with a person or premises under investigation for either the prosecution of a serious offence or to give effect to a mutual assistance request. In addition, clause 24 elaborates on the substantive grounds that must be provided in an application for such a warrant. Furthermore, as opposed to other warrants issued under this Bill, a judge or magistrate must require a service provider to keep the warrant issued confidential. Clause 24 also provides the penalty applicable to any service provider that fails to comply with a warrant issued under clause 24.

2.31 Part 6 of the Bill provides for international cooperation.

2.32 Clause 25 of the Bill provides for general principles relating to international cooperation.

2.33 Clause 26 of the Bill provides that the offences under Parts 2 and 4 of the Bill are considered extraditable offences under the Extradition Act 2003.

2.34 Clause 27 of the Bill provides that the Government may, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings or might lead to a request for cooperation by the foreign State. In addition, clause 27 provides that before providing such information to a foreign State, the Government may request that the information be kept confidential and used only subject to specified conditions.

2.35 Clause 28 of the Bill provides that where the Mutual Assistance in Criminal Matters Act 1997 is not applicable to a foreign State, the Government may require a foreign State to *inter alia* keep information provided by the Government confidential. In addition, clause 28 provides that any such request made on behalf of Fiji must be made

only by or with the authority of the Attorney-General.

2.36 Clause 29 of the Bill provides that subject to any limitation specified in Part 6 of the Bill, a foreign government, foreign agency or international agency may request the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of data stored by means of a computer system, located within Fiji or control of the Government. Clause 29 also provides that such a request must be in respect of data which the foreign government, foreign agency or international agency intends to submit a request for mutual assistance for *inter alia* the search of similar access of the data. In addition, clause 29 provides for the items that must be specified in a request for preservation and that upon receiving such a request, the Attorney-General or 24/7 network must take all appropriate measures to facilitate the request accordingly.

2.37 Clause 30 of the Bill provides for when the investigating agency discovers that a service provider in another State was involved in the transmission of communications during the execution of a request relating to a specified communication. Essentially, in situations like this, clause 30 provides that the Attorney-General or 24/7 network must expeditiously disclose to the requesting foreign government, foreign agency or international agency a sufficient amount of traffic data to identify that service provider and the path through which the specified communication was transmitted.

2.38 Clause 31 of the Bill provides for mutual assistance regarding accessing stored computer data. Subject to any limitations specified, a foreign government, foreign agency or international agency may request the investigating agency to order or *inter alia* search or similarly access data stored by means of a computer system located within Fiji, including data that has been preserved pursuant to clause 29. In addition, clause 31 outlines the items that must be included in a request for mutual assistance regarding accessing stored computer data and that upon receipt of such a request, the investigating agency must take all appropriate measures to obtain the necessary authorisation (including any warrants) to execute the request accordingly.

2.39 Clause 32 of the Bill provides that a police officer or other authorised person may access stored computer data if it is publicly available irrespective of where the data is located or if lawful consent is obtained.

2.40 Clause 33 of the Bill provides for mutual assistance regarding the real-time collection of traffic data. Clause 33 provides that a foreign government, foreign agency or international agency may request the Attorney-General to order or provide assistance in real-time collection of traffic data associated with specified communications in Fiji transmitted by means of a computer system. In addition, clause 33 provides the specific items that must be included in such a request. Clause 33 also provides that upon receiving such a request, the Attorney-General must take all appropriate measures to obtain necessary authorisation (including any warrants) to execute the request in accordance with Part 5 of the Bill.

2.41 Clause 34 of the Bill provides that a foreign government, foreign agency or international agency may request the Attorney-General to order or provide assistance in the real-time collection or recording of content data or specified communications transmitted by means of a computer system in the territory of Fiji. Clause 34 also elaborates on the items that must be specified in a request for assistance. In addition,

clause 34 provides that the Attorney-General must, if the request is in relation to an offence punishable with at least 5 years imprisonment, take all appropriate measures to obtain necessary authorisation (including any warrants) to execute the request accordingly.

2.42 Clause 35 of the Bill empowers the Minister responsible for communications to designate a point of contact or '24/7 network', who must be available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Clause 35 also provides that the point of contact must be properly resourced and that the point of contact also has the authority to coordinate and enable access to international mutual assistance under the Bill.

2.43 Part 7 of the Bill provides the miscellaneous provisions.

2.44 Clause 36 of the Bill empowers the Minister responsible for communications (**'Minister'**) to make regulations to prescribe matters that are required or permitted by the Bill to be prescribed or are necessary or convenient to be prescribed for carrying out or giving effect to the Bill and generally for achieving the purposes of the Bill. Clause 36 of the Bill also empowers the Minister to make regulations prescribing offences and penalties not exceeding, in the case of an individual a fine of $50,000 or imprisonment for a term of 15 years or both, or in the case of a body corporate a fine of $200,000.

3.0 MINISTERIAL RESPONSIBILITY

3.1 The Bill comes under the responsibility of the Minister responsible for communications.

A. SAYED-KHAIYUM
Attorney-General