THE REPUBLIC OF KIRIBATI

Arrangement of Sections

PART IV – PROCEDURAL LAW

PART V—INTERNATIONAL COOPERATION

PART VI – MISCELLANEOUS

THE REPUBLIC OF KIRIBATI

(No.10 of 2021)

I assent,

Beretitenti

21/09/ 2021

AN ACT

entitled

AN ACT TO PROVIDE FOR THE PREVENTION, INVESTIGATION AND SUPPRESSION OF COMPUTER RELATED OFFENCES AND FOR OTHER CONNECTED PURPOSES.

Commencement date:
2021

MADE by the Maneaba ni Maungatabu and assented to by the Beretitenti

PART I - PRELIMINARY

1. Short title

This Act may be cited as the Cybercrime Act 2021.

2. Commencement

This Act commences on a date that the Minister may by notice appoint.

3. Definitions

In this Act, unless the context otherwise requires—

'access' in relation to a computer system means to instruct, communicate with, store computer data in, receive computer data from, or otherwise make use of any of the resources of the computer system;

'child' shall mean any person under the age of 18 years;

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

'computer program' means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

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

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

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

'hinder' means modification of the contents of any computer system takes place if, by the operation of any function of the computer system concerned or any other computer system, or any act which impairs the normal operation of any computer system, and any act which contributes towards causing such a modification shall be regarded as causing it;

'interception' includes but is not limited to the acquiring, viewing and capturing of any computer data during transmission by technical means;

'material' includes, but is not limited to, any texts, images, audio, video and any other computer data;

'Minister' means the Minister responsible for Information and Communication;

'person's private part' means male and female genitals, including buttocks and female breasts;

'search and seize' means—
(a) activating and/or securing access on any onsite computer system and computer data;
(b) making and/or retaining a copy of computer data, including by using onsite equipment;
(c) maintaining the integrity of the relevant stored computer data;
(d) rendering inaccessible, or removing, computer data in the accessed computer system;
(e) taking a printout of a computer data; or
(f) seize and/or secure a computer system and/or part of it and/or a computer data;

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

'sexually explicit conduct' means—
(a) sexual intercourse; or
(b) any other activity of a sexual or indecent nature that involves the human body, or bodily actions or functions (whether or not that activity involves physical contact between people);

'sexual abuse material depicting a child' means any material that depicts—
(a) a child engaged in sexually explicit conduct;
(b) a person appearing to be a child engaged in sexually explicit conduct; and
(c) (c) realistic images representing a child engaged in sexually explicit conduct;

'subscriber's 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 by which can be established—
(a) the type of communication service used, the technical provisions taken thereto 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; and
(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

'secure access' a person secures access to any computer program or computer data held in a computer system if by causing a computer system to perform any functions that—
(a) alters or erases the computer program or computer data;
(b) copies or moves it to any computer data storage medium other than that in which it is held or to a different location in the computer data-storage medium in which it is held;

(c) uses it; or
(d) causes it to be output from the computer system in which is held (whether by having it displayed or in any other manner), and references to access to a computer program or computer data (and to an intent to secure such access) shall be read accordingly.

For the purpose of (c) in this definition, a person uses a computer program if the function they cause the computer system to perform: cause the computer program to be executed or is itself a function of the computer program. For the purpose of (d) in this definition, the form in which any computer program or computer data is output (and in particular whether or not it represents a form in which, in the case of a computer program, it is capable of being executed or, in the case of computer data, it is capable of being processed by a computer system) is immaterial;

'traffic data' means computer data that—
(a) relates to a communication by means of a computer system; and
(b) is generated by a computer system that formed a part in the chain of communication; and
(c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.

4. Application of this Act

This Act applies to:

(1) Act or omission done or made in the territory of the Republic of Kiribati; and
(2) Act or omission done or made—
  (a) on a ship or aircraft registered in the Republic of Kiribati; or
  (b) by a national of the Republic of Kiribati outside the territory of the Republic of Kiribati if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or
  (c) by a national of the Republic of Kiribati in any place or elsewhere.

PART II – ESTABLISHMENT OF A CYBERCRIME UNIT

5. Cybercrime Unit

(1) There shall be a Cybercrime Unit within the Kiribati Police Service consisting of Police officers whose function is to administer this Act.
(2) The Unit shall provide a report of its investigations to the Office of the Attorney General.
(3) Regulations may provide for—
  (a) composition of the Unit;
  (b) appointments;
  (c) qualifications;
  (d) terms of office and
  (e) rules or procedure of the investigation.

6. 24/7 Network

(1) The Cybercrime Unit shall be a point of contact available on a twenty-four hour, sevenday-a-week basis.
(2) The Unit shall provide assistance including facilitating, carrying out the following measures—
  (a) the provision of technical advice;
  (b) preservation of computer data pursuant to request from the requesting countries.
  (c) the collection of evidence, the provision of legal information, and locating of suspects.
(3) The Unit shall have the capacity to carry out communications with the point of contact of other countries on an expedited basis. The Unit shall work collaboratively with the Office of the Attorney-General for international mutual assistance or extradition on an expedited basis.
(4) The Unit shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

PART III – OFFENCES AND PENALTIES

7. Unauthorised access

(1) Access of any kind by any person to any computer program or computer data held in a computer system is illegal or unauthorised if that person—
  (a) is not entitled to control access of the kind in question to the computer program or computer data; and
  (b) does not have consent to access by him of the kind in question to the computer program or computer data from any person who is so entitled.
(2) Any person who knowingly, or recklessly and without authority causes a computer system to perform any function for the purpose of securing access to that computer system or computer data held in any computer system is liable on conviction to a fine not exceeding $10,000 or to imprisonment not exceeding 7 years or to both.
(3) For the purpose of this section, it is immaterial that the act in question is not directed at any particular—
  (a) computer program or computer data of any kind; or
  (b) computer program or computer data held in any computer system.

8. Unauthorised interception

(1) A person who knowingly or recklessly and without authority intercepts or attempts to intercept a non-public transmission by technical means of—
  (a) a computer data to, from or within a computer system; or
  (b) electromagnetic emissions from a computer system,
commits an offence punishable upon conviction, to a fine not exceeding $10,000 or imprisonment for a period not exceeding 7 years, or to both.
(2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular—
  (a) computer program or computer data of any kind; or

(b) computer program or computer data held in any computer system.

9. Unauthorised data interference

(1) A person who, knowingly or recklessly, and without authority—
- (a) damages or deteriorates computer data;
- (b) deletes computer data;
- (c) alters computer data;
- (d) renders computer data meaningless, useless or ineffective;
- (e) obstructs, interrupts or interferes with the lawful use of computer data;
- (f) obstructs, interrupts or interferes with any person in the lawful use of computer data; and
- (g) denies access to computer data to any person authorised to access it,

commits an offence punishable upon conviction, to a fine not exceeding $20,000 or imprisonment for a period not exceeding 10 years, or to both.

(2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular—
- (a) computer program or computer data of any kind; or
- (b) computer program or computer data held in any computer system.

10. Unauthorised system interference

(1) A person who, knowingly or recklessly, and without authority hinders or interferes with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data commits an offence punishable upon conviction, to a fine not exceeding $20,000 or imprisonment for a period not exceeding 10 years, or to both.

(2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular—
- (a) computer program or computer data of any kind; or
- (b) computer program or computer data held in any computer system.

11. Misuse of computer systems and computer program

Any person commits an offence who without authority, knowingly or recklessly produces, sells, possess, procures for use, imports, distributes or otherwise makes available—
- (a) a computer system or computer program designed or adapted primarily with the intent to committing an offence; or
- (b) a password, access code or similar computer data by which a computer may be accessed, with the intent that it be used to commit an offence,

is punishable upon conviction, to a fine not exceeding $10,000 or imprisonment for a period not exceeding 7 years, or to both.

12. Computer-related forgery

A person who knowingly or recklessly and without authority, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic computer data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the computer data is directly readable and intelligible commits an offence punishable upon conviction, to imprisonment for a period not exceeding 7 years.

13. Computer-related fraud

A person who knowingly or recklessly, and without authority causes a loss of property to another person by—

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

(b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, the penalty shall be imprisonment for a period not exceeding 7 years.

14. Sexual abuse material depicting a child

(1) A person who knowingly:

(a) produces sexual abuse material depicting a child—

(b) offers or makes available sexual abuse material depicting a child through a computer system;

(c) distributes or transmits sexual abuse material depicting a child through a computer system;

(d) procures or obtains sexual abuse material depicting a child through a computer system for oneself or for another person;

(e) possesses sexual abuse material depicting a child in a computer system or on a computer-data storage medium; or

(f) obtains access, by means of a computer system to sexual abuse material depicting a child,

commits an offence punishable upon conviction, to imprisonment for a period not exceeding 10 years.

(2) It is a defence to a charge of an offence under subsection (1) (b), (c), (d), (e) and (f) if the person establishes that the sexual abuse material depicting a child was a bona fide law enforcement purpose. If sexual abuse material depicting a child was stored for such a purpose, the authorised person needs to ensure that it is deleted as soon as it is not legally required anymore.

15. Solicitation of children

A person, who through the use of a computer system, communicates to a child, with the intent of committing an offence, including but not limited to;

(a) soliciting a child;

(b) grooming a child; and

(c) grooming a third party

for the purposes of engaging in a sexual explicit conduct with a child commits an offence punishable upon conviction to imprisonment for a period not exceeding 10 years.

16. Disclosure of details of an investigation

A service provider who receives a Court order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligations is stated by law and that service provider knowingly and without authority or in excess of authorisation, discloses—

(a) the fact that an order has been made; or
(b) anything done under the order; or
(c) any computer data collected or recorded under the order, commits an offence punishable, upon conviction, by imprisonment for a period not exceeding 5 years or a fine not exceeding $7,000 or to both.

17. Sending or publishing information or material by means of computer system

A person who knowingly and without authority sends or publishes, by means of a computer system any material exposing any person's private part whether dead or alive, commits an offence punishable upon conviction, to a fine not exceeding $3,000 or to imprisonment for a period not exceeding 2 years or to both.

18. Harassment utilising means of computer system

A person who initiates any communication by means of a computer system with the intent to coerce, intimidate, harass, or cause emotional distress to a person, which can result in endangering a person's life, commits an offence punishable upon conviction, to a fine not exceeding $3,000 or to imprisonment for a period not exceeding 2 years or to both.

19. Parties to offences

When an offence is committed, each of the following persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say—

(a) every person who knowingly aids or abets another person in committing the offence; and
(b) any person who counsels or procures any other person to commit the offence.

20. Offences by a body corporate

(1) A body corporate commits an offence if an employee, agent or officer of the body corporate knowingly commits an offence under this Act to the benefit of that body corporate—

(a) as a representative of the body corporate;
(b) carrying out duties of such responsibility that the person's conduct may fairly be assumed to represent the policies of the body corporate;
(c) with authority to exercise control within that body corporate; and

(d) where the offence was made possible due to the lack of supervision or control of a person referred to in paragraphs (a), (b) or (c).

(2) An offence committed by a body corporate is punishable by a fine not exceeding $50,000

(3) An employee, agent or officer is guilty of and liable to the penalty provided for that offence.

21. Admissibility of electronic evidence

In proceedings for an offence against any other laws, the fact that evidence has been generated from a computer system does not prevent that evidence from being admissible.

PART IV – PROCEDURAL LAW

22. Search and seizure

(1) If a Court on application by a police officer, is satisfied that there are reasonable grounds to suspect that there may be in a place, a computer system or computer data—
(a) that may be material as evidence in proving an offence under this Act; or
(b) any other criminal offences committed by means of a computer system;
(c) that has been acquired by a person as a result of an offence,

a Court may issue a warrant authorising a police officer, with such assistance as may be necessary to enter the place to search and seize the thing or computer data including search or similarly access:
(i) a computer system or part of it and a computer data stored within; and
(ii) a computer-data storage medium in which computer data may be stored in the territory of the country.

(2) Any person who exercises 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;
(b) give a copy of that list to the Director of Public Prosecutions;
(c) the occupier of the premises; and
(d) the person in control of such computer system.

(3) A police officer may refuse to give access or provide copies to the service provider or the owner if he or she has reasonable grounds to believe 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; or
(ii) another ongoing investigation; or
(iii)any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

(4) If a police officer who is undertaking a search based on subsection (1), has grounds to believe that the computer data sought is stored in another computer system or part of it

in its territory, and such computer data is lawfully accessible from or available to the initial computer system, he or she shall be able to expeditiously extend the search or similar accessing to the other computer system.

(5) A police officer who is undertaking a search is empowered to seize or similarly secure computer data accessed according to subsections (1) or (2).

23. Assistance

(1) A person who is not a suspect of a crime but is in possession or control of a computer system or computer data that is the subject of a search under section 22 shall permit, and assist if required by the police officer making the search to—
(a) access and use a computer system or computer data;
(b) obtain and copy that computer data;
(c) use a computer system to make copies; and
(d) obtain an intelligible output from a computer system in a format that can be read.

(2) A person who refuses to provide assistance under subsection (1) commit an offence and is liable fine not exceeding $3,000 or to imprisonment not exceeding 2 years or to both.

24. Production order

If a Court on application by a police officer is satisfied that a person or service provider has in his possession or have control of a computer data in, on or of a computer system required for the purpose of a criminal investigation or criminal proceedings, it may order that person or service provider to provide that specified computer data or subscriber information.

25. Expedited preservation

(1) Where a police officer is satisfied that—
(a) the specified computer data including content data and traffic data is reasonably required for the purpose of a criminal investigation; and
(b) there is a risk that the computer data including content data and traffic data may be destroyed or rendered inaccessible,
a police officer may write a notice to a person or a service provider in control of the computer system, ordering the person to ensure that the computer data, content data, traffic data and their integrity specified in the notice be preserved and maintained for a period of up to 60 days.

(2) Any person who is served with a written notice (subsection 1) shall comply with the content of such notice. Failure to comply with the notice amounts to an offence punishable to 2 years imprisonment or $3,000 fine or both.

(3) A police officer may extend the notice to a period not exceeding 100 days.

26. Partial disclosure of traffic data

If a Police officer is satisfied that specified traffic data stored in a computer system is required for the purpose of a criminal investigation or criminal proceedings, the Police

officers may order on a written notice the disclosure of sufficient traffic data about a specified communication to identify—

(a) the service providers; and

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

27. Collection of traffic data

If a Court on application by a police officer is satisfied that a person is engaged in conduct which may contravene this Act or constitute any other criminal offences committed by means of a computer system, a Court may issue a warrant authorising a police officer to:

(a) collect or record through the application of technical means; and

(b) compel a service provider, by written notice to that person or service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to assist the Police officer by all means to facilitate an investigation in the collection or recording of traffic data, in real-time, associated with specified communications transmitted in Kiribati by means of a computer system.

28. Interception of content data

If a Court on application by a police officer is satisfied that the content data of a communication is required for the purposes of a criminal investigation, a Court may issue a warrant authorising a police officer to:

(a) collect or record through the application of technical means; and

(b) compel a service provider or a person, within its existing technical capability:

(i) to collect or record through the application of technical means, or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in Kiribati transmitted by means of a computer system.

29. Condition and safeguards for protection of rights

(1) The execution of powers and roles under this Act are subject to conditions and safeguards provided for under the Constitution and human rights obligations pursuant to applicable International Conventions.

(2) Procedural safeguards for a child:

(a) Proceeding for an offence against this Act must not be commenced without the consent of the Attorney-General if the defendant was under 18 at the time he or she allegedly engaged in the conduct constituting the offence.

(b) However, a person may be prosecuted for, charged with, or remanded in custody in connection with, such an offence before the necessary consent has been given.

PART V—INTERNATIONAL COOPERATION

30. Cooperation with foreign Government

(1) The Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the following purposes—
  (a) investigations or proceedings concerning offences related to computer systems;
  (b) computer data, including content data and traffic data;
  (c) the collection of evidence in electronic form of an offence;
  (d) obtaining expeditious preservation and disclosure of traffic data or content 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 provision under this Act.

(2) Subject to the ***Mutual Assistance in Criminal Matters Act 2003***, the Attorney General may—
  (a) make requests on behalf of Kiribati to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Kiribati, 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 or security of Kiribati 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 Kiribati; or
    (iv) postpone action on a request if such action would prejudice an investigation or proceeding in Kiribati.

31. Mutual Assistance Act not applicable

(1) Where the Mutual Assistance Act is not applicable to a foreign State, the Government may require the 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 Kiribati to a foreign State for assistance under this provision must be made only by or with the authority of the Attorney-General.

32. Request in relation to the expeditious preservation of data

(1) Subject to any limitations specified in this Part, a foreign government, foreign agency or any international agency may make a request to the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of a computer data, located within Kiribati or under the 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 computer 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 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) On receiving the request under subsection (1), the Attorney-General or 24/7 network must take all appropriate measures to preserve expeditiously the specified computer 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 of 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 computer data and following the receipt of such a request, the computer data must continue to be preserved until a final decision is taken on the request.

33. Disclosure of service provider for transmission of specified communication

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.

34. Request for assistance from the investigating agency

(1) Subject to any limitations specified by the Government, a foreign government, foreign agency or international agency may request the investigating agency to search or similarly access, seize or similarly secure, and disclose the computer data located

within Kiribati, including the computer data that has been preserved pursuant to section 32.

(2) A request for mutual assistance regarding accessing 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 Kiribati, 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 Kiribati 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 specified computer system to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in Kiribati;
(i) give details of the stored computer data or computer 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 system;
(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) On receiving the request under subsection (1), the investigating 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) On obtaining necessary authorisation including any warrants to execute the request, the investigating agency may seek the support and cooperation of the foreign government, foreign agency or international agency during the search and seizure.

(5) On conducting the search and seizure request the investigating 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.

35. Mutual assistance regarding real-time collection of traffic data

(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 Kiribati 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) On 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) On 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) On 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.

36. Extradition

The offences under this Act are extraditable offences under the laws relating to Extradition.

PART VI – MISCELLANEOUS

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

A Police officer may, without authorisation:
(a) access publicly available stored computer data, regardless of where the computer data is located geographically; or
(b) access or receive, through a computer system, stored computer data located in other Jurisdictions, if the Police officer obtains the lawful and voluntary consent of a

person who has the lawful authority to disclose the computer data through that computer system.

38. Act to have overriding effect

The provisions of this Act shall have effect even if there is anything inconsistent contained in any other law for the time being in force.

39. Copyright infringement

Any person who knowingly breaches the copyright of another person by means of computer system, commits an offence and shall be liable to punishment under the laws related to Copyright.

40. Confidentiality

(1) A service provider or person involved in an investigation of an offence in this Act, must not disclose any information related to the investigation to any person except when required to do so by any court of law or under any law.
(2) A person who contravenes subsection (1) commits an offence and is liable to a fine not exceeding $3,000 or to imprisonment not exceeding 2 years or to both.

41. Regulations

The Minister may make regulations, prescribing all matters that are necessary or convenient to be prescribed for carrying out or giving effect to the provisions in this Act.

42. Consequential amendments

Section 94, Part XIV of the Communications Act 2013 and sections 24 to 35 of the Communication (Amendment) 2017 are hereby repealed.

The Cybercrime Act 2021

Explanatory Memorandum

This Cybercrime Act 2021 implements the Government of Kiribati's Information Communication Technology (ICT) policy for strengthening the legislative framework on cyber-space. This Act aims to harmonise the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime, provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form and setting up a fast and effective regime of international cooperation.

The Cybercrime Act 2021 was developed to align with the Budapest Convention on Cybercrime with the intent to join the convention in the future.

Part I – Preliminary Matters

Part I covers Section 1 to Section 4 of the Cybercrime Act 2021. Part I includes definitions and terminologies used throughout the Act, it also covers the applicability of the Act; setting out jurisdictional boundaries for which this Act can be executed.

Part II – Establishment of a Cybercrime Unit

Part II covers Section 5 to Section 6 of the Cybercrime Act 2021 which calls for the establishment of a cybercrime unit within the Kiribati Police Service (KPS), and that this unit will administer this Act and also function as a 24/7 focal contact point for international cooperation on cybercrime investigations.

Part III – Offences and Penalties

Part III sets out general offences and penalties under the Act. Part III covers Section 7 to Section 21 of the Cybercrime Act 2021. It is an offence under the Act to:

1. access any computer system without authority;
2. intercept non-public transmissions without authority;
3. damage, delete or alter computer data without authority;
4. interfere with the functioning of a computer system by altering or suppressing a computer data without authority;
5. sell, possess, procure, import or distribute:
    a. a computer system or computer program designed for the purpose of committing a crime;
    b. a password, access code or similar computer data for use in committing an offence;
6. change a computer data to forge any material through a computer system e.g. birth certificate, school certificate, … etc.
7. produce, offer or make available, have in possession or access sexual abuse material depicting a child without authority;
8. solicit a child for sexual explicit conduct;
9. disclose details of an investigation without authority;

10. send or publish through a computer system any material exposing any person's private part without authority;
11. initiate a communication to coerce, intimidate, harass, or cause emotional distress to a person resulting in endangering a person's life;
12. aid or abet or assist in any way any person committing any offence under this Act;

Offences made by a Body Corporate will be charged to the Body Corporate and the officer who execute the act constituting the offence.

Part II also established recognition and admissibility of electronic evidences.

Part IV – Procedural Law

Part IV covers Section 22 to Section 29 of the Cybercrime Act. Part IV sets out the following procedural powers: search and seizure of computer data; seeking assistance for the purpose of investigating an offence; production of a court order; expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; collection of traffic data; and interception of content data. Part IV ends with common conditions and safeguards, applicable to all procedural powers in Part IV.

The conditions and safeguards set out limit of these procedural powers which are subjected to safeguards and conditions provided for under the Constitution and human rights obligation pursuant to relevant International Convention. It also established the need for the Attorney General consent when a defendant is a child prior any proceedings for an offence committed by a child.

Part IV also set out the need for a Court order for more intrusive procedural powers when investigating any offence under this Act. Section 27 and 28 requires a Court to issue a warrant to collect or record traffic data and intercepting content data.

Part V International Cooperation

Part V covers Section 30 to Section 36 of the Cybercrime Act 2021. Part V set out mutual assistance and international collaboration regimes for Kiribati and foreign governments or entities on Cybercrime investigations. This part also establishes provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between Kiribati and any requesting parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Act. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Part IV. The provision for mutual assistance is also subjected to the Mutual Assistance in Criminal Matters Act 2003.

Part V also set out that all offences under this Act are extraditable offences and is also subjected to relevant laws covering extradition.

Part VI – Miscellaneous

Part VI covers Section 37 to Section 42 of the Cybercrime Act. Part VI set out miscellaneous powers and provisions. These provisions include a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available).

It also covers an overriding effect provision if there are provisions within this Act that may be inconsistent in any other law.

This part also establishes copyright infringement offence which is subjected to the relevant Copyright law. It also covers an offence for breach of confidentiality of an investigation.

Part VI also establishes the powers of the Minister in prescribing all matters that are necessary for carrying out this Act, including making regulations under this Act.

Part VI also repeals Section 94, Part XIV of the Communications Act 2013 and Sections 24 to 35 of the Communication (Amendment) 2017.

CERTIFICATE OF THE CLERK OF THE MANEABA NI MAUNGATABU

This printed impression of the Cybercrime Act 2021 has been carefully examined by me with the Bill which passed the Maneaba ni Maungatabu on the 23rd August 2021 and is found by me to be a true and correctly printed copy of the said Bill.

.....

Eni Tekanene
Clerk of the Maneaba ni Maungatabu

Published by exhibition at the Maneaba ni Maungatabu this 21..... day of .....September..... 2021.

.....

Eni Tekanene
Clerk of the Maneaba ni Maungatabu