Pacific regional workshop on cybercrime legislation (Tonga, 27-29 April 2011)

# Review of cybercrime legislation in Pacific States

Alexander Seger / Cristina Schulman
Council of Europe,
Strasbourg, France
alexander.seger@coe.int
cristina.schulman@coe.int

www.coe.int/cybercrime

1

## Legislative responses to cybercrime: What is required?

Criminalising conduct + Tools for efficient investigations – and safeguards + Efficient international cooperation

*Harmonisation*

= The Budapest Convention on Cybercrime as a solution

Council of Europe

Legislation on cybercrime 2

2

## Budapest Convention as a „model law“

- Use as a checklist
- Compare provisions
- Use wording

| Provision of Convention | Provision in national law |
|---|---|
| Art 4 System interference | ? |
| Art 6 Misuse of devices | ? |
| Art 9 Child pornography | ? |
| Art 16 Expedited preservation | ? |
| Art 18 Production order | ? |

Council of Europe



3

## 1 Definition of terms

Defining key terms in legislation:

- “Computer system”
- “Computer data”
- “Service provider”
- “Traffic data”

Council of Europe



4

## Article 1 of the Convention on Cybercrime:

1 Definition of terms

➢"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

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

## Tonga Computer Crimes Act 2003

Art 2:

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

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



## Article 1 of the Convention on Cybercrime:

1 Definition of terms

➢"service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service

➢"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 communication's origin, destination, route, time, date, size, duration, or type of underlying service

## Tonga Computer Crimes Act 2003, Art 2:

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

➢"traffic data" means computer data that relates to a communication by means of a computer system; and is generated by a computer system that is part of the chain of communication, and shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

# 2 Substantive Criminal Law

**Legislation to deal with – as a minimum:**

- **Illegal access to a computer system** ("hacking", circumventing password protection, key-logging, exploiting software loopholes etc.)
- **Illegal interception** (violating privacy of data communication)
- **Data interference** (malicious codes, viruses, Trojan horses etc.)
- **System interference** (hindering the lawful use of computer systems)
- **Misuse of devices** (tools to commit cyber-offences)
- **Computer-related forgery** (similar to forgery of tangible documents)
- **Computer-related fraud** (similar to real life fraud)
- **Child pornography**
- **Infringement of copyright and related rights**

*Criminalising specific techniques/technologies or conduct?*

Council of Europe





# Article 2 of the Convention: illegal access

➢Establish as criminal offences under domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

## Tonga Computer Crimes Act 2003

**4 Illegal access**

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

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

| Country |
|---|
| Cook I. |
| Fiji Sec 340, 343 |
| FSM |
| Kiribati |
| Marshalls |
| Nauru |
| Niue |
| PNG |
| Palau |
| Samoa |
| Solomon I. |
| Tonga a |
| Tuvalu |
| Vanuatu |

Council of Europe

## Article 3 of the Convention: illegal interception

- Establish as criminal offences under domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

| Country |
|---|
| Cook I. |
| Fiji |
| FSM |
| Kiribati |
| Marshalls |
| Nauru |
| Niue |
| PNG |
| Palau |
| Samoa |
| Solomon I. |
| Tonga |
| Tuvalu |
| Vanuatu |

### Tonga Computer Crimes Act 2003

7 Illegal interception of data

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

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

b) electromagnetic emissions from a computer system that are carrying computer data, commits an offence and shall be liable upon conviction, to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.





## Article 4 of the Convention: data interference

- Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

| Country |
|---|
| Cook I. |
| Fiji |
| FSM |
| Kiribati |
| Marshalls |
| Nauru |
| Niue |
| PNG |
| Palau |
| Samoa |
| Solomon I. |
| Tonga |
| Tuvalu |
| Vanuatu |

### Tonga Computer Crimes Act 2003

5 Interfering with data

A person who, willfully or recklessly without lawful excuse:

a) destroys or alters data;

b) renders data meaningless, useless or ineffective;

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

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

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

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

# Article 5 of the Convention: system interference

- Establish as criminal offences under domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

## Tonga Computer Crimes Act 2003

**6 Interfering with computer system**

A person who wilfully or recklessly, without lawful excuse:

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

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

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

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |





# Article 6 - Misuse of devices

1 Establish as criminal offences under domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or available of:

i a device, including a computer program, designed or adapted p committing any of the offences established in accordance with th 5;

ii a computer password, access code, or similar data by which computer system is capable of being accessed, with intent that it committing any of the offences established in Articles 2 through 5

b the possession of an item referred to in paragraphs a.i or ii above for the purpose of committing any of the offences established Party may require by law that a number of such items be possess attaches.

2 This article shall not be interpreted as imposing criminal liability where the pr use, import, distribution or otherwise making available or possession referred is not for the purpose of committing an offence established in accordance w Convention, such as for the authorised testing or protection of a computer syst

3 Each Party may reserve the right not to apply paragraph 1 of this article, provid concern the sale, distribution or otherwise making available of the items refer article.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

# Article 6 - Misuse of devices

## Tonga Computer Crimes Act

Council of Europe

**8 Illegal devices**

**(1) A person who:**

**willfully or recklessly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available:**

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

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

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

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

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

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





# Article 7 - Computer-related forgery

Council of Europe

- **Establish as criminal offences under domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.**

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Article 8 - Computer-related fraud

➢Establish as criminal offences under domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

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

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.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |





## Article 9 - Child pornography

1 Establish as criminal offences when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

## Article 9 - Child pornography



2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Article 9 - Child pornography



**Tonga** CRIMINAL OFFENCES (AMENDMENT) ACT 2003

"115A Child pornography
(1) Any person who, wilfully in any manner —
(a) publishes child pornography;
(b) produces child pornography for any purpose; or
(c) possesses child pornography:
commits an offence punishable, upon conviction.....

(3) For the purposes of this section —
(a) the expression "child pornography" includes material that visually depicts —
(i) a child engaged in sexually explicit conduct;
(ii) a person who appears to be a child engaged in sexually explicit conduct; or
(iii) images representing a child engaged in sexually explicit conduct;
(b) the expression "child" means a person under the age of 14 years; for the purpose of doing an act referred to in subsection (1)."

## Article 10 - Copyright and related rights



1 Establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Break-out session



**Group 1**
Cooks, Niue, Tonga,Tuvalu
Faciliators: Andrew, Loraine

**Group 2**
Fiji, Samoa, PNG, Solomons,Vanuatu
Facilitators: Kate, Alexander

**Group 3**
FSM, Kiribati, Marshalls, Nauru, Palau
Facilitor: Siaosi

## Task:

**Discuss measures/steps to be taken at domestic level to fully implement provisions equivalent to:**

Definitions (Art. 1)

**Substantive law**

Illegal access (Art. 2)
Illegal interception (Art 3)
Data interference (Art. 4)
System interference (Art. 5)
Misuse of devices (Art. 6)
Forgery (Art. 7)
Fraud (Art. 8)
Child pornography (Art. 9)
Copyright and related rights (Art. 10)

# 3 Procedural Law

Council of Europe

**Legislation to provide for – as a minimum:**

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards





## Article 14 – Scope of procedural provisions

Council of Europe

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.

## Electronic evidence:

## Tonga:

**EVIDENCE (AMENDMENT) ACT No. 21 of 2003**
**"54A General admissibility**
**Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the ground that it is an electronic record.**

**54B Scope**
**54C Authentication**
**54D Best evidence rule**
**54E Presumption of integrity54F Standards**
**54G Proof by affidavit**
**54H Agreement on admissibility**
**54I Admissibility of electronic signature**





## Article 15 - Conditions and safeguards

1 Each Party shall ensure that ... the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

## Article 16 of the Convention – Expedited preservation of stored computer data



1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

### Tonga Computer Crimes Act

Sec. 13 Preservation of data

(1) Where any police officer is satisfied that:

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

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

the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

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

| Country | Commer |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Article 17 - Expedited preservation and partial disclosure of traffic data



1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Article 18 - Production order



1 ...measures to empower competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

3 For the purpose of this article, the term "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 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;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | Section 13? |
| Tuvalu | |
| Vanuatu | |





## Article 19 - Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Measures to ensure that where authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

## Article 19 - Search and seizure of stored computer data



3 Measures to empower competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Measures to empower competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Tonga Computer Crimes Act 2003



### Sec. 9 Search and seizure warrants

(1) If a magistrate is satisfied on sworn evidence that there are reasonable grounds to suspect that there may be in a place a computer, computer system, computer data or data storage medium which:
(a) may be material evidence in proving an offence; or
(b) has been acquired by a person as a result of an offence;
the magistrate may issue a warrant authorizing any police officer, with such assistance as may be necessary, to enter the place to search and seize the computer, computer system, computer data or data storage medium.
(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable:
(a) make a list of what has been seized, with the date and time of seizure; and
(b) give a copy of that list to —
(i) the occupier of the premises; or
(ii) the person in control of the computer system.
(3) Subject to subsection (4), on request, any police officer or another authorized person shall:
(a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or
(b) give the person a copy of the computer data.
(4) The police officer or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies may —
(a) constitute a criminal offence; or
(b) prejudice:
(i) the investigation in connection with which the search was carried out;
(ii) another ongoing investigation; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

# Article 20 - Real-time collection of traffic data

1 measures to empower competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

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

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 measures to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

| Country |
|---|
| Cook I. |
| Fiji |
| FSM |
| Kiribati |
| Marshalls |
| Nauru |
| Niue |
| PNG |
| Palau |
| Samoa |
| Solomon I. |
| Tonga |
| Tuvalu |
| Vanuatu |





# Tonga Computer Crimes Act 2003

## Sec. 15 Interception of traffic data

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

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

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

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

## Article 21 - Interception of content data



1 Measures, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, 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 its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Measures to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

| Country |
|---|
| Cook I. |
| Fiji |
| FSM |
| Kiribati |
| Marshalls |
| Nauru |
| Niue |
| PNG |
| Palau |
| Samoa |
| Solomon I. |
| Tonga |
| Tuvalu |
| Vanuatu |



## Tonga Computer Crimes Act 2003



### Sec. 14 Interception of electronic communications

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

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

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

## Break-out session

### Group 1
Cooks, Niue, Tonga,Tuvalu
Faciliators: Andrew, Loraine

### Group 2
Fiji, Samoa, PNG, Solomons,Vanuatu
Facilitators: Kate, Alexander

### Group 3
FSM, Kiribati, Marshalls, Nauru, Palau
Facilitor: Siaosi

## Task:
**Discuss measures/steps to be taken at domestic level to fully implement provisions equivalent to:**

- Scope (Art. 14)
- Safeguards and conditions (Art. 15)
- Expedited preservation (Art. 16)
- Expedited preserv. & partial disclosure (Art. 17)
- Production order (Art. 18)
- Search and seizure (Art 19)
- Real-time collection traffic data (Art. 20)
- Interception content data (Art. 21)



# 4 International Cooperation

## Chapter III of the Convention - International cooperation

### Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Chapter III - International cooperation
## Section 2 – Specific provisions

### Art 29 - Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party 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 paragraph 1 shall 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 Party 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.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |





### Art 30 - Expedited disclosure of preserved computer data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Art 31 - Mutual assistance regarding accessing stored computer data

4 International cooperation

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Art 32 - Trans-border access to stored computer data (public/with consent)

4 International cooperation

A Party may, without the authorisation of another Party:

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

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

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Art 33 - Mutual assistance in real-time collection of traffic data

4 International cooperation

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Art 34 - Mutual assistance regarding interception of content data

4 International cooperation

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |

## Art 35 - 24/7 network



1 Each Party shall 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. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
a the provision of technical advice;
b the preservation of data pursuant to Articles 29 and 30;
c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

| Country | Comment |
|---|---|
| Cook I. | |
| Fiji | |
| FSM | |
| Kiribati | |
| Marshalls | |
| Nauru | |
| Niue | |
| PNG | |
| Palau | |
| Samoa | |
| Solomon I. | |
| Tonga | |
| Tuvalu | |
| Vanuatu | |



## Break-out session



**Group 1**
Cooks, Niue, Tonga,Tuvalu
Faciliators: Andrew, Loraine

**Group 2**
Fiji, Samoa, PNG, Solomons,Vanuatu
Facilitators: Alexander

**Group 3**
FSM, Kiribati, Marshalls, Nauru, Palau
Facilitor: Siaosi, Kate

## Task:

**Discuss measures/steps to be taken to enhance international cooperation, including:**

- Implementation of international cooperation provisions of chapter III of Budapest Convention + accession
- 24/7 contact points (art 35 Budapest)
- Application of existing treaties and bi- or multilateral agreements
- Police to police cooperation
- Judicial cooperation/MLA