CARICOM SUBMISSION

CONTRIBUTIONS TO THE SECOND NEGOTIATING SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR CRIMINAL PURPOSES

CHAPTER 1 – GENERAL PROVISIONS

ARTICLE: GENERAL PROVISIONS

The purpose**s** of this Convention are as follows:

1. To promote and strengthen measures aimed at preventing and combatting crimes and other unlawful actions directed against the confidentiality, integrity and availability of Information and Communication Technology systems and computer data more efficiently and effectively;

2. To promote, facilitate and support international cooperation and technical assistance to prevent and combat criminal offences and other unlawful actions directed against the confidentiality, integrity and availability of Information and Communication Technology systems and computer data.

3. To promote, facilitate and support international cooperation and technical assistance in the recovery of assets resulting from criminal offences and other unlawful actions referred to in this Convention**.**

ARTICLE: SCOPE OF APPLICATION

1. In accordance with its provisions, this Convention shall apply to the prevention, investigation and prosecution of criminal offences, to the promotion, facilitation and support of international cooperation in preventing and combating the use of Information and Communications Technologies for criminal offences, and to the freezing, seizure, confiscation and return of the proceeds of such offences established in accordance with this Convention.

2. For the purposes of implementing this Convention, it shall not be necessary, except as otherwise stated therein, for the criminal offences established pursuant to its provisions to result in damage or harm to persons, property and the State**.**

ARTICLE: PROTECTION OF SOVEREIGNTY

1. State parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereignty, sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States Parties or States.

2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State Party or State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State Party or State in accordance with its domestic law and in accordance with international law and obligations.

CHAPTER 2 - CRIMINALIZATION

ARTICLE: ILLEGAL / UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS OR DATA

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences when committed intentionally and without right, the access to the whole or any part of a computer system. A State Party may require that the offence is committed where there is a breach or infringement of a security measure or 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. (Based on Budapest Convention Article 2 – Illegal access)

ARTICLE: ILLEGAL/ UNAUTHORIZED INTERCEPTION

1. Each State Party shall adopt such legislative and other measures as are necessary to establish as a criminal offence, when committed intentionally, the interception without right or authority of a computer system or data, where such interception is done by technical means to intercept traffic data and data processed by means of Information Communication Technology which is not intended for public use, including electromagnetic emissions from a computer system carrying such computer data.

2. *A State Party may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system.*

ARTICLE: ILLEGAL DATA INTERFERENCE

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the inputting, damaging, deletion, deterioration, alteration or suppression of computer data without right or authority.

2. A State Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

ARTICLE: ILLEGAL SYSTEM INTERFERENCE

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right or authority, the hindering of the functioning of an Information and Communication Technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

2. Each State Party may reserve the right to impose an aggravation of penalty where the actions as outlined in paragraph 1 involve or affect critical infrastructure.

ARTICLE: MISUSE OF DEVICES/ MALICIOUS SOFTWARE/ COMPUTER PROGRAM.

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right:

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

      i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the criminal offences established in accordance with Articles (Unauthorized/ Illegal Access,

Unauthorized/ Illegal Interception/ Data Interference/ System Interference).

ii. a computer password, access code, or similar data by which the whole or any part of an information, communication and technology system is capable of being accessed, with intent that it be used for the purpose of committing any of the criminal offences established in Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference); and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the criminal offences established in Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference). A State Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This Article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing a criminal offence established in accordance with Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference) of this Convention, such as for the authorised testing or protection of a computer system.

3. Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a)(ii) of this Article.

ARTICLE: CONTENT – RELATED OFFENCES

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right, the following conduct:

a) Producing child sexual exploitation and abuse material through an information and communication technology system;

b) Offering or making available child sexual exploitation and abuse material through an information and communication technology system;

c) Distributing or transmitting child sexual exploitation and abuse material through an information and communication technology system;

d) Procuring child sexual exploitation and abuse material through a computer system/ information and communication technology system for oneself or for another person;

e) Possessing child sexual exploitation and abuse material in a computer system/ information and communication technology system or on a computer -data storage medium.

2. For the purposes of paragraph 1 above, the term "child sexual exploitation and abuse material" shall include material that visually depicts:

a) A child engaged in sexually explicit conduct;

b) A person appearing to be a child engaged in sexually explicit conduct;

c) Realistic images representing a minor engaged in sexually explicit conduct.

3. For the purposes of paragraph 2 above, the term "child" means every human being below the age of eighteen (18) years unless under the law applicable to the child, majority is attained earlier. (Convention on the Rights of the Child, Article 1)

ARTICLE: VIOLATION OF PRIVACY/NON-CONSENSUAL DISTRIBUTION OF SEXUAL IMAGES

1. Each State Party shall adopt such legislative and other measures as are necessary to establish as a criminal offence, when committed intentionally and without right, the following conduct;

a) Knowingly publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct;

b) The publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person is done with the intention to harass or cause harm to the person depicted in the image;

Definition of intimate image

2. In this Article, "intimate image" means a visual recording of a person made by any means including a photographic, film or video recording;

a) In which the person is nude**,** is exposing his or her genital organs or anal region or breasts, or the person is engaged in explicit sexual activity;

b) In respect of which, at the time of recording, there were circumstances that gave rise to a reasonable expectation of privacy; and

c) In respect of which the person depicted continues to have a reasonable expectation of privacy at the time the offence is committed.

ARTICLE: INTELLECTUAL PROPERTY

Each State Party shall adopt such legislative and other measures as are necessary to establish as criminal offences the infringement of copyright and related rights, as defined by the legislation of the State Party, when such acts are wilfully committed by means of Information and Communication Technology, and on a commercial scale.

COMPUTER RELATED OFFENCES

ARTICLE - Computer Related Forgery

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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.

2. A State Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

ARTICLE - Computer Related Fraud

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right or authority, the causing of a loss of property to another person by:

    a) Any input, alteration, erasure or suppression of computer data;

    b) Any interference with the functioning of a computer system;

With fraudulent or dishonest intent of procuring an economic benefit for oneself or for another person.

ARTICLE: INCOHATE OFFENCES

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences participation in any capacity such as an accomplice, assistant, instigator, abettor or conspirator in an offence established in accordance with this Convention.

2. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence any attempt to commit an offence established in accordance with this Convention.

3. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, the preparation for an offence established in accordance with this Convention.

ARTICLE: LIABILITY OF LEGAL PERSONS

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the commission of a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as a part of an organ of the legal person, who holds a leading position within it, by virtue of:

    a) A power of representation of the legal person;

    b) An authority to take decisions on behalf of the legal person;

c) An authority to exercise supervision or control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this Article, each State Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its express or implied authority.

3. Subject to the domestic law of the State Party, the liability of legal persons may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the criminal offences.

5. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

ARTICLE: SANCTIONS AND MEASURES

1. Each State Party shall make the commission of a criminal offence established in accordance with this Convention liable to sanctions that are commensurate to the gravity of that offence, and are effective, proportionate and dissuasive, including the deprivation of liberty.

2. Each State Party shall ensure that legal persons held liable in accordance with Article (Liability of Legal Persons) shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

CHAPTER 3 – PROCEDURAL MEASURES & LAW ENFORCEMENT

ARTICLE: - SCOPE OF PROCEDURAL PROVISIONS

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

2. Except as otherwise provided in Article (Interception of Communication), each State 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 – (the Criminalization provisions) of this Convention;

   b) Other criminal offences committed by means of a information, communication and technology system; and

   c) The collection of evidence in electronic form of a criminal offence.

3. Each State Party may reserve the right to apply the measures referred to in Article (Real Time Collection of Data) only to criminal offences or categories of criminal offences specified in the reservation, provided that the range of such offences is not more restricted than the range of criminal offences to which the State Party applies the measures referred to in Article (Interception of Content Data).

4. Where a State Party due to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in Article (Real Time Collection of Data) and Article (Interception of Content Data) to communications being transmitted within a computer system of a service provider, which system:

   (i) Is being operated for the benefit of a closed group of users, and

   (ii) Does not employ public communications networks and is not connected with another computer system, whether public or private,

   That State Party may reserve the right not to apply those measures to such communications.

5. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles (Real Time Collection of Data and Interception of Content Data).

ARTICLE: CONDITIONS & SAFEGUARDS

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Article are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments.

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 State Party shall consider the impact of these powers and procedures in this Article upon the rights, responsibilities and legitimate interests of third parties.

ARTICLE: EXPEDITED PRESERVATION OF COMPUTER DATA

1. Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly expeditiously obtain, collect and preserve specified computer data, including traffic data, in particular where there are grounds for believing that the data is particularly vulnerable to deletion, modification or loss;

2. Where a State Party gives effect to paragraph 1 above by means of an order to a person, including to a legal person, to preserve specified stored computer data in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to require that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, but no longer than the period determined by the domestic law of that State Party, to enable the competent authorities to seek disclosure of the data. A State Party may provide for such an order to be subsequently renewed.

3. Each State Party shall adopt such legislative and other measures as may be necessary to require the person who is tasked with preserving the information to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this Article shall be established in accordance with the Articles (Scope of Procedural Provisions and Conditions & Safeguards).

ARTICLE: EXPEDITED PRESERVATION AND PARTIAL DISCLOSURE OF TRAFFIC DATA

1. Each State Party shall adopt, in respect of traffic data that is to be preserved under the Article (EXPEDITED PRESERVATION OF COMPUTER DATA), 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 are involved in the transmission of that communication; and

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

2. The powers and procedures referred to in this article shall be subject to Articles (Scope of Procedural Provisions & Conditions and Safeguards).

ARTICLE: PRODUCTION ORDER

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to order:

    a) A person, including to a legal person, in its territory to submit 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 that territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be established in accordance with Articles (Scope of procedural provisions and Conditions & Safeguards)

3. For the purpose of this Article, the term "subscriber information" shall mean any information held by a service provider relating to subscribers to its services other than traffic data or content data, on the basis of which it is possible to establish:

a) The type of information and communications services used, the technical provisions taken and the period of service;

b) The subscriber's identity, postal or geographic addresses, telephone and other access numbers, including IP addresses and billing and payment information, available in the service agreement or arrangement;

c) Information relating to the location of information and telecommunications equipment that has a bearing on the service agreement or arrangement.

ARTICLE: SEARCH AND SEIZURE OF INFORMATION STORED OR PROCESSED ELECTRONICALLY

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to search or similarly access:

a) Information and Communication Technology system or part of it and computer data stored therein; and

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

2. Each State Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have reasonable 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 expeditiously to extend the search or similar accessing to the other system.

3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its 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. Each State Party shall adopt such legislative and other measures as may be necessary to empower its 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, 2 and 3.

5. The powers and procedures referred to in this Article shall be subject to Articles (Scope of Procedural Provisions & Conditions & Safeguards).

ARTICLE: REAL TIME COLLECTION OF TRAFFIC DATA

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to:

    a) collect or record through the application of technical means in 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 in 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 State Party, in accordance with its domestic law, 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 in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to require 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 (Scope of Procedural Provisions & Conditions & Safeguards).

ARTICLE: INTERCEPTION OF DATA

1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious criminal offences to be determined by domestic law, to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to:

a) Collect, record or store through the application of technical means in the territory of that Party, and
b) compel a service provider, within its existing technical capability:

i. to collect, record or store through the application of technical means in 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 State Party, in accordance with its domestic law, 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 in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to require 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 (Scope of Procedural Provisions & Conditions and Safeguards).