Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version May 2008
[Reformat January 2011]

Cybercrime legislation – country profile

BARBADOS

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Barbados**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs	**Section 3 of the *Computer Misuse Act, 2005-4* defines the same terms identified in Article 1 of the Cyber Crime Convention.** "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 programme,

automatic processing of data; b "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; c "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; d "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	facilitates communication, 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 programme suitable to cause a computer system to perform a function. "service provider" means *(a)* a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and *(b)* any other entity that processes or stores computer data on behalf of that entity or those users. "traffic data" means computer data that (a) relates to a communication by means of a computer system; (b) is generated by a computer system that is part of a chain of communication; and (c) shows the origin, destination, route, time, date, size, duration of the communication of the type of underlying services used to generate the data.
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its 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.	**Illegal Access-** Section 4 of the Computer Misuse Act, 2005-4 (1) A person who knowingly or recklessly, and without lawful excuse or justification, (a) gains access to the whole or any part of a computer system; (b) causes a programme to be executed; (c) uses the programme to gain access to any data; (d) copies or moves the programme or data (i) to any storage medium other than that in which that programme or data is held; or (ii) to a different location in the storage medium in which that programme or

	data is held; or (e) alters or erases the programme or data is guilty of an offence and is liable on conviction on indictment to a fine of $25 000 or to imprisonment for a term of 2 years or to both. (2) For the purposes of subsection (1), the form in which any programme is obtained or copied and, in particular, whether or not it represents a form in which it is capable of being executed, is immaterial.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its 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.	**Illegal Interception- Section 7 of the Computer Misuse Act, 2005-4** **7.** A person who knowingly and without lawful excuse or justification intercepts by technical means *(a)* any transmission to, from or within a computer system that is not available to the public; or *(b)* electromagnetic emissions that are carrying computer data from a computer system is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Interfering with data- Section 5 of the Computer Misuse Act, 2005-4** 5. (1) A person who knowingly or recklessly, and without lawful excuse or justification, (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 the data; is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both. (2) Subsection (1) applies whether the person's act is of temporary or permanent effect.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the	**Interfering with Computer Systems- Section 6 of the *Computer Misuse Act, 2005-4*** 6. A person who knowingly or recklessly, and without lawful excuse or justification,

functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	(a) hinders the functioning of a computer system by (i) preventing the supply of electricity, permanently or otherwise, to a computer system; (ii) causing electromagnetic interference to a computer system; (iii) corrupting the computer system by any means; (iv) adding, deleting or altering computer data; or (b) interferes with the functioning of a computer system or with person who is lawfully using or operating a computer system is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, 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 offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; 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 offences established in Articles 2 through 5. A 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 an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.	**Illegal Devices- Section 8 of the Computer Misuse Act, 2005-4** 8. A person who knowingly or recklessly, and without lawful excuse or justification, *(a)* supplies, distributes or otherwise makes available (i) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence under section 4, 5, 6 or 7; or (ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7; or *(b)* has an item mentioned in paragraph *(a)*(i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7 is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

3 Each 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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its 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.	**Access with the intention to commit an offence- Section 9 of the Computer Misuse Act, 2005-4** 9. A person who knowingly uses a computer to perform any function in order to secure access to any programme or data held in that computer or in any other computer with the intention to commit an offence involving property, fraud or dishonesty is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its 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.	**Access with the intention to commit an offence- Section 9 of the Computer Misuse Act, 2005-4** 9. A person who knowingly uses a computer to perform any function in order to secure access to any programme or data held in that computer or in any other computer with the intention to commit an offence involving property, fraud or dishonesty is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution	**Child pornography- Section 13 of the *Computer Misuse Act, 2005-4*** 13. (1) A person who, knowingly, *(a)* publishes child pornography through a computer system; or *(b)* produces child pornography for the purpose of its publication through a computer system; or

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. 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.	*(c)* possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication is guilty of an offence and is liable on conviction on indictment, (i) in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or (ii) in the case of a corporation, to a fine of $200 000. (2) It is a defence to a charge of an offence under subsection (1)(i) or (ii) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose. (3) For the purposes of subsection (1), *(a)* "child pornography" includes material that visually depicts (i) a minor engaged in sexually explicit conduct; or (ii) a person who appears to be a minor engaged in sexually explicit conduct; or (iii) realistic images representing a minor engaged in sexually explicit conduct; *(b)* "publish" includes (i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; (ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(a)*; or (iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(a)*.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to 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.	**Access with the intention to commit an offence- Section 9 of the Computer Misuse Act, 2005-4** 9. A person who knowingly uses a computer to perform any function in order to secure access to any programme or data held in that computer or in any other computer with the intention to commit an offence involving property, fraud or dishonesty is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

2 Each Party shall adopt such legislative and other measures as may be necessary to 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. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Section 17 of the *Criminal Procedure Act, Cap 127* provides for aiding and abetting. This section is read into all legislation.**

Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: 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 control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each 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 authority. 3 Subject to the legal principles of the Party, the liability of a legal person 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 offence.	The *Computer Misuse Act, 2005-5* addresses 'a person' which would include a legal person. However, it is noted that in section 13 which speaks to child pornography it addresses corporate liability in relation to child pornography. In addition section 18 **(Production of data for criminal proceedings)** which speaks to Production Orders also provides a specific penalty for corporations.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 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. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 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 Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of 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.	The *Computer Misuse Act, 2005-4* is in accordance with the requirements under Article 15 of the Cyber Crime Convention in regard to the application of certain conditions safeguards the nature of the procedure or power concerned, *inter alia*, including judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

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 – 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. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data 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 subject to Articles 14 and 15.	**Preservation of data for criminal proceedings- Section 20 of the *Computer Misuse Act, 2005-4*** 20. (1) Where a police officer satisfies a Judge on the basis of an *ex parte* application that *(a)* data stored in a computer system is reasonably required for the purposes of a criminal investigation; and *(b)* there is a risk that the data may be destroyed or rendered inaccessible, the Judge may make an order requiring the person in control of the computer system to ensure that the data specified in the order be preserved for a period of up to 14 days. (2) The period may be extended beyond 14 days where, on an *ex parte* application, a Judge authorises an extension for a further specified period of time.
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	**Order for disclosure of data- Section 19 of the *Computer Misuse Act, 2005-4***

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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	19. Where a Judge is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify *(a)* the Internet service providers; and *(b)* the path through which the communication was transmitted.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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.	**Production of data for criminal proceedings**- Section 18 of the *Computer Misuse Act, 2005-4* 18. (1) Where a Judge is satisfied on the basis of an application by a police officer that specified computer data or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that *(a)* a person in control of a computer system produce from the computer system specified computer data or other intelligible output of that data; and *(b)* an Internet service provider in Barbados produce information about persons who subscribe to or otherwise use the service. (2) A person referred to in paragraph *(a)* or *(b)* of subsection (1) who makes an unauthorised disclosure of any information under his control is guilty of an offence and is liable on conviction on indictment, *(a)* in the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or *(b)* in the case of a corporation, to a fine of $200 000.

Article 19 – Search and seizure of stored computer data	**Search and seizure- Section 15 of the *Computer Misuse Act, 2005-4***
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 Each 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 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. 3 Each 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 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 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary. (2) A warrant issued under this section may authorise a police officer to *(a)* seize any computer, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed; *(b)* inspect and check the operation of any computer referred to in paragraph *(a)*; *(c)* use or cause to be used any computer referred to in paragraph *(a)* to search any programme or data held in or available to such computer; *(d)* have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer into readable and comprehensible format or text, for the purpose of investigating any offence under this Act; *(e)* convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system; *(f)* make and retain a copy of any programme or data held in the computer referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computers. (3) A warrant issued under this section may authorise the rendering of assistance by an authorised person to the police officer in the execution of the warrant. (4) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both. (5) For the purposes of this section, "authorised person" means a person who has the relevant training and skill in computer systems and technology who is identified, in writing, by the Commissioner of Police or a gazetted officer

	designated by the Commissioner as authorised to assist the police; "encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data; "plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary 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, 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 Each Party shall adopt such legislative and other measures as may be necessary 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.	**Assisting a police officer**-**Section 16 of the *Computer Misuse Act, 2005-4*** 16. (1) A police officer executing a warrant in accordance with section 15 is entitled to require a person who is in possession or control of a computer data storage medium or computer system that is the subject of the search to assist him or an authorised person to *(a)* access and use a computer system or computer data storage medium to search any computer data available to or in the system; *(b)* obtain and copy computer data referred to in paragraph *(a)*; *(c)* use equipment to make copies; *(d)* obtain access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence; and *(e)* obtain an intelligible output from a computer system in a plain text format that can be read by a person. (2) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both. (3) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version. **Record of seized data to be provided to the owner** -**Section 17 of the *Computer Misuse Act, 2005-4***

	17. (1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 15, the person who made the search shall, at the time of the search or as soon as practicable after the search, *(a)* make a list of what has been seized or rendered inaccessible, 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. (2) Subject to subsection (3), a police officer or authorised person shall, on request, *(a)* permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or *(b)* give the person referred to in paragraph *(a)*, a copy of the computer data. (3) The police officer or authorised person may refuse to give access to or provide copies of computer data referred to in subsection (2) if he has reasonable grounds for believing that giving the access or providing the copies *(a)* would constitute a criminal offence; or *(b)* would prejudice (i) the investigation in connection with which the search was carried out; or (ii) another investigation connected to the one in respect of which the search was carried out; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, 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	**Assisting a police officer-Section 16 of the *Computer Misuse Act, 2005-4*** 16. (1) A police officer executing a warrant in accordance with section 15 is entitled to require a person who is in possession or control of a computer data storage medium or computer system that is the subject of the search to assist him or an authorised person to *(a)* access and use a computer system or computer data storage medium to search any computer data available to or in the system; *(b)* obtain and copy computer data referred to in paragraph *(a)*; *(c)* use equipment to make copies;

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 Each Party shall adopt such legislative and other measures as may be necessary 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.	*(d)* obtain access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence; and *(e)* obtain an intelligible output from a computer system in a plain text format that can be read by a person. (2) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 18 months or to both. (3) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version. - **Record of seized data to be provided to the owner** -**Section 17 of the *Computer Misuse Act, 2005-4*** 17. (1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 15, the person who made the search shall, at the time of the search or as soon as practicable after the search, *(a)* make a list of what has been seized or rendered inaccessible, 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. (2) Subject to subsection (3), a police officer or authorised person shall, on request, *(a)* permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or *(b)* give the person referred to in paragraph *(a)*, a copy of the computer data. (3) The police officer or authorised person may refuse to give access to or provide copies of computer data referred to in subsection (2) if he has reasonable grounds for believing that giving the access or providing the copies *(a)* would constitute a criminal offence; or

	(b) would prejudice (i) the investigation in connection with which the search was carried out; or (ii) another investigation connected to the one in respect of which the search was carried out; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations..
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Section 2-Application** The *Computer Misuse Act* applies to an act done or an omission made *(a)* in Barbados; *(b)* on a ship or aircraft registered in Barbados; or *(c)* by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed.
Chapter III – International co-operation	
Article 24 – Extradition	Extradition Act, Cap 189

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its	

instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible 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. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence	Mutual Assistance in Criminal Matters Act, Cap. 140A

of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	Section 18(1) of the Mutual Assistance in Criminal Matters Act, Cap. 140A
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate	The Mutual Assistance in Criminal Matters Act, Cap. 140A will have to be amended to speak to the requirements set out under Article 27 of the Cyber Crime Convention.

to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance 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 it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of	

the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	Section 19 and First Schedule to Schedule, paragraph 3(a) to the Mutual Assistance in Criminal Matters Act, Cap. 140A The First Schedule to Schedule to the Mutual Assistance in Criminal Matters Act, Cap. 140A in paragraph 3(a) states that a request for assistance in obtaining evidence shall give details of the procedure that the country wishes to be followed in giving effect to the request, including details of the manner and form in which any evidence or information is to be supplied to that country. However it must be noted that this provision only applies to requests from Commonwealth countries.

Article 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. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused 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	**Preservation of data for criminal proceedings-Section 20 of the Computer Misuse Act, 2005-4** Mutual Assistance in Criminal Matters Act, Cap. 140A NB: Dual criminality requirement applies except under Part IVA which only relates the CARICOM Member States.

interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic 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.	**Order for disclosure of data-Section 19 of the Computer Misuse Act, 2005-4** Mutual Assistance in Criminal Matters Act, Cap. 140A NB: Dual criminality requirement applies except under Part IVA which only relates the CARICOM Member States.
Article 31 – Mutual assistance regarding accessing of stored computer data 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:	Mutual Assistance in Criminal Matters Act, Cap. 140A

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.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available 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.	Mutual Assistance in Criminal Matters Act, Cap. 140A
Article 33 – Mutual assistance in the real-time collection of traffic data 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.	Mutual Assistance in Criminal Matters Act, Cap. 140A
Article 34 – Mutual assistance regarding the interception of content data 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.	Mutual Assistance in Criminal Matters Act, Cap. 140A
Article 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	Section 3(1) of the Mutual Assistance in Criminal Matters Act, Cap. 140A states that the Attorney-General is the Central Authority. As the Central Authority the Attorney-General would be the 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

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.	in electronic form of a criminal offence in accordance with Article 35 of the Cyber Crime Convention.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	