Establishment of Harmonized Policies for the ICT Market in the ACP countries

Electronic Evidence: Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Electronic Evidence:

Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. This report has not been through editorial revision.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate the Caribbean region's economic integration and thereby its greater prosperity and social transformation, the Caribbean Community (CARICOM) Single Market and Economy has developed an ICT strategy focusing on strengthened connectivity and development.

Liberalisation of the telecommunication sector is one of the key elements of this strategy. Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalisation are not to be so various as to constitute an impediment to the development of a regional market.

The project 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) has sought to address this potential impediment by bringing together and accompanying all 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonised ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), the project has been undertaken in close cooperation with the Caribbean Telecommunications Union (CTU), which is the chair of the HIPCAR Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation - EuropeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. HIPCAR has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the region were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, which reflect country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example for other regions to follow as they too seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication Union (CTU) Secretariat for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008. It is a companion document to the Model Policy Guidelines and Legislative Texts on this HIPCAR area of work[1].

In response to both the challenges and the opportunities of information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP", as a component of the Programme "ACP-Information and Communication Technologies (@ACP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: the Caribbean (HIPCAR), sub-Saharan Africa (HIPSSA) and the Pacific Island Countries (ICB4PAC).

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants including Ms. Pricilla Banner and Mr. Gilberto Martíns de Almeida, who prepared the initial draft documents. The documents were then reviewed, finalized and adopted by broad consensus by the participants at the First Consultation Workshop for HIPCAR's Working Group 1 on ICT Policy and Legislative Framework on Information Society Issues, held in Saint Lucia on 8-12 March2010. Based on the assessment report, Model Policy Guidelines and Legislative Texts were developed, reviewed and adopted by broad consensus by the participants at the Second Consultation Workshop held in Barbados on 23-26 August 2010.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries and regulators as well as their counterparts in the ministries of justice and legal affairs, academia, civil society, operators, and regional organizations, for their hard work and commitment in producing the contents of the HIPCAR model texts. The contributions from the Caribbean Community Secretariat (CARICOM) and the Caribbean Telecommunications Union (CTU) are also gratefully acknowledged.

Without the active involvement of all of these stakeholders, it would have been impossible to produce this document, reflecting the overall requirements and conditions of the Caribbean region while also representing international best practice.

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Cybersecurity (CYB) Division and Regulatory and Market Environment (RME) Division. Support was provided by Philip Cross of the ITU Area Office for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

[1] HIPCAR Model Policy Guidelines and Legislative Texts, including implementation methodology, are available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

Table of contents

Page

Section I:
Introduction

The emergence of the new technological landscape brought about by developments in Information and Communication Technologies has provided a platform for many forms of electronic interactions and communications between individuals, businesses, and governments. These interactions are varied in form and include business transactions or electronic commerce, electronic or distance learning or education, electronic government, online banking and communications, and several others. Technology therefore provides a new medium to facilitate traditional interactions with the attendant issues which arise from such interactions such as liability, breach of contract etc.

It is also the case, however, that the emergence of the new technological landscape has also seen an evolution of crime and criminality. These interactions, whether having to do with business transactions or with criminal activity, produce electronic evidence which must be properly harnessed in order to enforce legal rights or to prosecute criminals. Therefore, identifying electronic evidence and the manner in which it may maintain its integrity and be reliably harnessed and used as a tool in, for instance, prosecutions of computer misuse and cyber crimes is critical in this new technological landscape.

The impetus by states to introduce *electronic evidence* legislation or to amend existing evidence legislation to take into account electronic evidence is driven by the recognition that the traditional common law rules of evidence used to enforce civil rights and criminal law are inadequate in dealing with technological advances and therefore need to be modernized.[2] The nature of electronic evidence itself including its novelty and the fact that it may be seen as fragile and easily manipulated, poses challenges to countries in updating their laws. The fragility of electronic evidence means that it can be altered, damaged or destroyed by improper handling and improper examination. Electronic evidence is oftentimes also transnational in nature when servers are located in multiple countries which enhances the difficulty in using the evidence and having it properly admitted in a court of law.

In recognizing these difficulties, the Commonwealth Secretariat sought to introduce a Draft Model Law on Electronic Evidence to address the needs of small commonwealth jurisdictions which may not have the resources to conduct their own review. The Expert Group which was convened in 2000 for such purpose, examined the issue of admissibility of electronic evidence and the question whether the rules that apply to other forms of documentary evidence could be applied in a similar manner to electronic evidence. In view of the vulnerability of electronic records to manipulation in contrast to paper, the admissibility rule had to be re-fashioned to take account of the risk. This led to the adoption of the *system reliability test* as it was resolved that while it may be difficult to detect changes in an electronic document itself as opposed to alterations on paper, the test would not focus on the document itself but rather on the method or the system by which the document was produced. The Model law also focused on issues relating to the general admissibility rule, scope, authentication, the best evidence rule, the presumption of integrity, standards, proof by affidavit, cross-examination, agreement on admissibility of electronic records and admissibility of electronic signatures. The Model Law drew from the Singapore Evidence Act (Section 35), the Canada Uniform Electronic Evidence Act and UNCITRAL Model Law on E-Commerce.

[2] See: Commonwealth Secretariat Draft Model Law on Electronic Evidence as available at http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BE9B3DEBD-1E36-4551-BE75-B941D6931D0F%7D_E-evidence.pdf

The Commonwealth Secretariat decided that the complexity of the issue warranted a separate model law on electronic evidence to ensure admissibility of electronic evidence but did not rule out the decision by member states to use the Model law as an amendment to existing law on evidence or as part of electronic transactions law. While Belize has adopted in wholesale fashion the Model Law, other Beneficiary countries have sought to amend existing evidence legislation.

In 2002, the Commonwealth Secretariat made a recommendation that all commonwealth countries either adopt or adapt the model legislation as a Commonwealth model.

Since then, the rapid pace of technological progress and the increasing sophistication and dissemination of cybercrime have posed new challenges to countries interested in regulating electronic evidence. Cloud computing, cryptography, time stamping, electronic judicial proceedings, international standards, are examples of new items to be considered.

In such scenario, regulation on electronic evidence must be articulated in conjunction with the regulation on items such as expedited preservation of data, production order, search and seizure proceedings, data retention, and others, in order to provide required efficacy. ITU's documents "Understanding Cybercrime: Phenomena, Challenges and Legal Response", a Guide for Developing Countries"[3] are of particular interest in this regard.

[3] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Section II:
Executive Summary

This Assessment Report has been prepared in accordance with Phase 1 of Work Plan for the Working Group on ICT Legislative Framework – Information Society Issues under the HIPCAR Project, which makes provision for a critical assessment report of E-Evidences existing in a number of States (the "Beneficiary Member States"[4]) in the Caribbean Region. This Assessment Report is for discussion and adoption by the HIPCAR Working Group on ICT Legislative Framework Meeting to be held in Saint Lucia on March 8-13th, 2010.

The purpose of this Assessment Report is to provide an analysis of the key issues and common principles reflected in ICT regulatory and legislative frameworks relating to e-evidence in the Beneficiary Member States and to provide a reference document for policy makers, legislators and regulators in the Beneficiary Member States that will serve as a basis for harmonized policy guidelines to be developed in Phase II of the Work Plan, and that may be used to produce model legislation under Phase III of the Work Plan.

Section 3 of this Assessment Report briefly highlights the challenges inherent to legislating in the area of e-evidence, as well as the challenges posed by the task of harmonizing the legislative framework of electronic evidence in the Beneficiary Member States, given the varied legal and regulatory frameworks and the varied stages of development of ICT policy implementation and of e-evidence legislation.

Section 4 identifies the international and regional trends and best practices, which provide the basis for comparison with national laws, and eventual gap analysis.

Section 5 addresses an overview of current legislation in the Beneficiary Member States vis-à-vis the main issues associated with an effective legal framework for e-evidence.

Section 6 presents a comparative law analysis based on the international, regional, and national sceneries portrayed by Sections 4 and 5.

Section 7 shows a table picturing the current stage of legislative efforts in the Beneficiary Member Stages, including a matrix featuring the main issues associated with such endeavour. Grades attributed to legislation of each individual Beneficiary Member State are rooted in the comments made in Sections 5 and 6.

Section 8 analyses the main factors and criteria which may subsidy the definition and implementation of policy guidelines.

Examples ofthe most advanced pieces of legislation of individual Beneficiary Member States are attached in the Annexes.

[4] Antigua and Barbuda, The Bahamas, Barbados, Jamaica, the Commonwealth of Dominica, the Domincan Republic,Haiti, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago.

Section III: Challenges

The increasing dangers to the integrity, availability, confidentiality, authenticity, and authorship of electronic documents, associated with the actions of hackers, crackers, re-mailers, corporate frauds, and cybercrimes in general, have caused a great deal of concern regarding the risks and constraints for judicial admissibility of electronic evidence.

On the other hand, the proliferation of international standards and frameworks on information security and on governance of information technology, highly secure digital signature, time stamping techniques, and electronic Court proceedings, have generated a common impression that electronic evidence may be safer and more reliable than conventional, non-electronic evidence, provided a certain degree of care is accomplished.

Given such opposite trends and possibilities, regulating electronic evidence implies the need of striking a balance between technical and procedural aspects, in order to harness evidence at reasonable cost as well as to meet well-accepted principles such as the principle of equivalence between digital and non-digital evidence, the principle of precaution (which requires adoption of prevention or risk-reduction measures), and the principle of accreditation (which demands accredited certification of processes, to inspire greater level of confidence).

Computer forensics is of utmost importance for evaluating electronic evidence, especially with regard to cryptography, steganography and other techniques which may jeopardize the revelation of contents of some electronic documents.

Cloud computing – that is, the partitioning of data processing across different geographies – may aggravate current difficulties on establishing jurisdiction over practices perpetrated in any given two or more localities, as the production or the evaluation of electronic evidence may have to be shared among different venues.

Production and assessment of digital evidence may also face restraints where privacy rights and the principle of no self-incrimination are present. Interception of communication may be necessary in some circumstances, to provide the required evidence, and shall be balanced vis-à-vis privacy concerns. The “opening” of protected electronic files may demand disclosure of passwords by the accused party (or by a digital notary, i.e., digital signature certificate provider).

The high capacity of data storage has led to incredible amounts of data to go through discovery proceedings, so the massive quantity of data to be analysed, and the corresponding need of enough technical resources, is another complexity to be considered.

The different legal systems to which different countries are affiliated materialize additional complication for the tasks of enforcing rights and of harmonizing national laws. The Beneficiary Member States have varied legal and regulatory frameworks, and are at quite different stages in development and implementation of their ICT policies.

Although the Beneficiary Member States are parties to various relevant regional and international conventions, and in most cases are members of the Caribbean Community, there is no Regional Sovereign power with authority to make laws on their behalf as a group and to ensure compliance, as is the case in the European Community.

Section IV: International and Regional Trends and Best Practices

There is an expressive number of international, regional, and country laws and best practices associated with regulating electronic evidence. Some of them relate to electronic transactions or to electronic signature, others focus strictly on Court's admission, while a third group is concerned with cybercrime.

Besides UNCITRAL's Model Law, and Canada's and Singapore's benchmarks which have inspired the Commonwealth's Draft Model Law on Electronic Evidence, and the already mentioned ITU's Toolkit for Cybercrime Legislation (hereinafter, "ITU's Toolkit") and "Understanding Cybercrime: A Guide for Developing Countries" (hereinafter, "ITU's Guide"), the experiences of France, Germany, Italy, U.S.A., and Spain, as well as the Budapest Convention on Cybercrime and some European Directives, are worth mentioning.

France has taken the initiative of amending its Civil Code, by means of Law 2000-230, which incorporated references to electronic evidence in the sections pertaining to written evidence, and gave electronic evidence the same weight as of paper evidence, provided the electronic document can have its authorship and integrity properly confirmed.

Germany's law on digital signatures (Bundesgesetzblatt 1997 Teil I Seite 1872-6) has determined that the issuer of digital certificates documents its compliance with security measures required by said law, so that third parties can verify the integrity of procedures and data at any time, and has determined that such certifying authority provides time stamping to those interested in obtaining it.

The Italian government has enacted Decree n. 513, of November 10, 1997, and a Decree of the Council of Ministers of February 08, 1999, aiming at regulating the formation, recording, and transmission of "informatic and telematic instruments", whereby it has established that "informatic documents" are valid and binding once they meet the requirements specified therein.

The law of the State of Illinois, U.S.A., on security in the electronic commerce, has set forth that an electronic file is to be deemed secure whenever an advance security procedure has qualified it, in accordance with a commercially reasonable procedure under the circumstances, applied and invoked in good faith. The U.S.A. also has substantial production of Court definitions on computer terminology, which help determine the meaning of certain statutory provisions.

Spain has enacted the Royal Decree- Law 14/1999, on digital signatures, establishing the legal presumption that digital signature products which are in conformity with technical standards published in the Official Gazette of the European Community are secure, recognizing the effect of commonly accepted technical standards.

The samples above show how different national strategies can be in the pursuit of comprehensive strategies to address regulation of electronic evidence.

The Budapest Convention on Cybercrime has ruled, in Article 14, that "Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for" in that section for the purpose of specific criminal investigations or proceedings, and has then expressly mentioned "the collection of evidence in electronic form of a criminal offence." Therefore, in order to comply with the Budapest Convention, it is expected that electronic evidence are collected in the context of expedited preservation of computer data and of traffic data, production order, search and seizure, real-time collection of traffic data, and interception of content data.

Section IV

ITU's Toolkit provides valuable insights on how to regulate electronic evidence:

i) in Section 4, b, preservation of computer data, content data, or traffic data, for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of the country or of another jurisdiction to seek its disclosure; the integrity of such preserved data shall be documented by means of a mathematical algorithm and such record maintained along with the preserved data; competent authorities may request that the preservation order be renewed; the custodian and any other person ordered to preserve such data shall keep confidential;

ii) in the Explanatory Comments to Sample Legislative Language, on section 4.1 (Definitions): it defines "computer" based upon U.S. law and court decisions[5] interpreting the definition; it has also defined "computer data", explaining that it "includes the word "state" because digital 1s or 0s can be a value whose existence or lack of existence has external significance, such as on or off, present, absent, set, unset, etc.";

iii) in Section 4.2 (Substantive Provisions), it clarifies that to make "images" of computer data, content data or traffic data, in the context of search and seizure, e is to produce "a duplicate of an entire storage media whereas a copy is a duplication of the data or some subset of it";

iv) in Sections 14 and 15 (Preservation of Data), it points to the intention that preservation of computer data, content data, or traffic data be conducted in compliance with the European Telecommunications Standards Institute (ETSI) Technical Standards (TS) 102 656, Lawful Interception (LI): Retained Data.

ITU's Guide also provides important recommendations as well as references to best practices:

i) in Section 3.3.4 ("Developing Procedures for Digital Evidence"), it explains that digtal evidence is defined as "any data stored or transmitted using computer technology that supports the theory of how an offence occurred", and that the fragility of digital evidence is "especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down and therefore requires special preservation techniques, as well as that new developments can have great impact on dealing with digital evidence, for instance, cloud-computing, which causes that might be stored abroad and can only be accessed remotely, if necessary;

ii) also in Section 3.3.4, it stresses that collection of digital evidence is linked to computer forensics, which consists in systematic analysis of IT equipment with the purpose of searching for digital evidence, including "analysing the hardware and software used by a suspect, supporting investigators in identifying relevant evidence, recovering deleted files, decrypting files, and, Identifying Internet users by analysing traffic data".

[5] ITU's Toolkit quotes the following interesting court decisions: "In *GWR Medical, Inc. v. Baez,* 2008 U.S. Dist. LEXIS 19629, the court determined that a CD-ROM was not a computer because: [A] CD-ROM does not, in and of itself, process information. The CD-ROM is analogous to a compilation of documents and training materials, and cannot be considered a computer under the CFAA [Computer Fraud and Abuse Act] without processing capabilities. In *United States v. Mitra,* 405 F.3d 492, the court determined that a computer-based radio system that spread traffic across twenty frequencies and the radio units used the control channel to initiate a conversation with others on the network, was a computer. The prosecution argued that the radio trunking system was a computer because it contained a chip that performed high-speed processing in response to signals received on the control channel. The defendant, Mr. Mitra, claimed that even if the radio system contained a computer, that every cell phone, cell tower, iPod, and wireless baseless station would also be swept within the CFAA, and Congress surely did not intend the law to be so encompassing when it passed the law in 1984. The court, however, disagreed with this line of thinking, pointing out that legislators know that technology changes rapidly (...)"

Section IV

The different approaches revealed by international laws and best practices, including diverse scope, terminology, and strategies, point to the convenience of reflection on the most suitable framework to Beneficiary Member States, in the context of policy-making. Some aspects shall be considered in this regard, such as the inevitable connection between electronic evidence and related matters (digital signature, expedited preservation, data retention, production order, and others), existing international patterns of terminology and of procedures, and the need to face the new phenomena (cloud computing, cryptography, and others) which already pose effective challenges.

Section V: Overview of Electronic Evidence in Beneficiary Member States

As pointed out above, regulation of electronic evidence has not been contemplated by all Beneficiary Member States, and different paths have been followed by the ones which have already enacted laws or rulings on the matter, as described below.

5.1 Barbados

Barbados has not enacted a separate piece of legislation to deal with electronic evidence. However, the Evidence Act does contain certain provisions which deal with information recorded or stored by means of a computer or other device. The Act defined the term "document" to include information recorded or stored in, or derived from a computer. It also abolishes the "best evidence rule" with the effect that electronic evidence would not be excluded based on the fact that it is not the original document. The Barbados Act also makes provision for evidence produced by machines, devices or process. The Act specifies that where it is reasonably open to find the device or process is one that if properly used, ordinarily does what the party tendering the document asserts it to have done, it shall be presumed that (unless the contrary is proved) in producing the document on the occasion in question, the device or process did what the party asserts it to have done.

5.2 Belize

Belize is the only Beneficiary state to have enacted a separate Electronic Evidence Act, which fully follows the Commonwealth Model Law on Electronic Evidence. The Act defines "electronic record" to mean data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device and includes a display, print out or other output of that data. The term "computer" is not defined in the Act. The salient provisions of the Act include general admissibility of electronic records, issues of authentication, application of the best evidence rule, presumption of integrity, standards, proof of affidavit, cross-examination, agreement on admissibility of electronic records and admissibility of electronic signatures.

5.3 Jamaica

Jamaica has not enacted a self-contained Electronic Evidence legislation but it does have an Evidence Act with minimal provisions relating to the admissibility of electronic documents. The term "document" is defined in the Act to include *(a)* any map, plan, graph or drawing; *(b)* any photograph; *(c)* any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied *so* as *to* be capable (with or without the aid of some other equipment) of being reproduced therefrom; *(d)* any film (including microfilm), negative, tape or other device in which one or more visual images are embodied *so* as to be capable (with or without *the* aid of some other equipment) of being reproduced therefrom. The Act also provides in section 31 for the admissibility of computer evidence constituting hearsay as well as the admissibility of computer evidence not constituting hearsay.

5.4 Saint Vincent and the Grenadines

Saint Vincent and the Grenadines does not have a separate Electronic Evidence Act but has enacted an Electronic Transactions Act which has minimal provisions relating to the admissibility of electronic evidence. The Act provides for non-discrimination against electronic information and specifies that information shall not be denied legal effect, validity or enforcement solely on the ground that it is in electronic form. The term "information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the internet and wireless application protocol communications.

The Act also provides that in proceedings for an offence against a law of Saint Vincent and the Grenadines, the fact that (a) it is alleged that an offence of interfering with an information system has been committed; and (b) evidence has been generated from that information system does not of itself prevent that evidence from being admissible. Electronic signature is al provided for in the Act. The provision specifies that an electronic signature is not without legal force and effect merely on the ground that it is in electronic form.

5.5 Trinidad and Tobago

Trinidad and Tobago does not have a separate Electronic Evidence Act but some provisions relating to the admissibility of electronic documents can be found in the Evidence Act, Cap. 7:02. The terms "computer" is defined in the Act to mean "any device for storing or processing information and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or other process." The term "document" is also defined in the Act to include any disc, tape, sound track or other device in which sounds or other data, not being visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom. The Act makes provision for admissibility in civil proceedings of statements produced by computers as well as admissibility of certain trade or business records. The Act also makes provision for the admissibility of computer records in criminal cases.

5.6 The Bahamas

The Bahamas does not have, specifically, a Electronic Evidence Act, but some provisions relating to the admissibility of electronic documents can be found in the Electronic Communications and Transactions Act, of 2003, in its Parts II ("Legal Recognition and Functional Equivalency of Electronic Communications, Signatures, Contracts and related matters") , III ("Intermediaries and E-Commerce Service Providers") and IV ("E-Commerce Advisory Board"). These Parts of the Act focus on the civil and criminal liability of ISPs, Court acceptance of electronic documents, and creation of a Board to advice the Telecommunications Ministry on such matters. The Act also provides several definitions, concepts and standards applicable to the E-Evidence matters.

Section VI:
Comparative Law Analysis

6.1 Definitions

Despite the fact that only Belize has a separate legislation dealing with Electronic Evidence, there exist some commonalities in respect of the terminology used in the Acts of Beneficiary Member States which address admissibility of electronic documents to some degree.

6.1.1 "Computer"

Of the Beneficiary states under review, Trinidad and Tobago is the only state to define the meaning of "computer" in its Evidence Act. In the Act, "computer" means any device for storing and processing information. One must note that this definition is not the same as that used in the Computer Misuse Act of Trinidad and Tobago wherein computer is defined to be "an electronic, optical, electrochemical, or a magnetic, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices."

Recommendations:

Where the term "computer" is used in Evidence legislation it should be defined for purposes of certainty. Furthermore, the definition of computer should correspond as much as possible to the definition of the term in related legislation for the purpose of consistency and harmony. The definition shall differentiate between "computer" and "computer device", and make reference to both, where appropriate.

6.1.2 "Document" or "Electronic Record"

The definition of document is contained in the Barbados, Jamaica and Trinidad and Tobago Evidence Acts. On the other hand, the Belize and The Bahamas Acts makes reference to an "electronic record".

In the Barbados Act, the term "document" is defined to include (a) anything on which there is writing; (b) a map, plan, drawing or photograph; and (c) any information recorded or stored by means of any tape recorder, computer or other device, and any material subsequently derived from the information so recorded or stored. This means that information recorded or stored by means of a computer and material derived from any information recorded or stored in a computer would be a document within the Act. The use of the term "document" is applicable to all legal proceedings including criminal and civil proceedings.

In the Evidence Act of Jamaica, a "document" is defined to include *(a)* any map, plan, graph or drawing; *(b)* any photograph; *(c)* any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied *so* as *to* be capable (with or without the aid of some other equipment) of being reproduced therefrom; and *(d)* any film (including microfilm), negative, tape or other device in which one or more visual images are embodied *so* as to be capable of being reproduced therefrom.

In the Trinidad and Tobago Evidence Act "document" includes any device by means of which information is recorded or stored. It also includes, in addition to a document in writing, *(a)* any map, plan, graph or drawing; *(b)* any photograph; *(c)* any disc, tape, sound track or other device in which sounds or other data, not being visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and *(d)* any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as mentioned above) of being reproduced therefrom.

As is clear from a review of the definitions, there is a level of harmonization between the provisions from Jamaica and Trinidad and Tobago in that each refers to a document as including either a device in which sounds or other data (not being visual images) are embodied *so* as *to* be capable (with or without the aid of some other equipment) of being reproduced or any device in which one or more visual images are embodied so as to be capable of being reproduced therefrom. However, the Barbados provision seems to be most suitable when making reference to a document as constituting electronic evidence. This is because in the former countries, visual images are excluded in (c) and in (d), hence the categories appear restrictive so as not to extend to images from a computer. The Barbados provision makes it clear, however, that a document includes any information recorded or stored by means of any tape recorder, computer or other device, and any material subsequently derived from the information so recorded or stored.

The Belize definition of an "electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device and includes a display, print out or other output of that data. An electronic records system on the other hand includes the computer system, or other similar device by or in which data is stored, and any procedures related to the recording and preservation of electronic records. The definition of electronic record is broad in scope and encompasses any data derived from a computer system.

Similarly to Belize's law, the Electronic Communications and Transactions Act from The Bahamas brings a broad definition of "electronic record", as being an "information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form".

Recommendations:

It is essential that Electronic Evidence legislation provide guidance as to the form of evidence to be adduced, whether in documentary form or otherwise. This is important to ensure certainty in the legislation as to what type of information or document constitutes electronic evidence. The provision should provide certainty and should be comprehensive enough to cover all types of information which may be recorded or stored in, or derived from, a computer system or an electronic records system. It is convenient to specify that document may include content data, traffic data, and location data, which are categories employed in laws which regulate matters connected with digital evidence. Given the fact that digital evidence are increasingly constituted by images, the definition of document shall not exclude images *per se*. The concept of images in electronic documents shall be differentiated from "imaging", the production of duplicates of documents in search and seizure proceedings.

6.1.3 "Legal Proceedings"

Both the Barbados and the Belize Acts define legal proceedings. In the Barbados Act both civil and criminal proceedings are specifically defined. In the Belize Act, "legal proceedings" means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

Section VI

Recommendations:

It is recommended that provision should be made for the admissibility of electronic documents or records in all proceedings, including, but not limited to, civil, criminal, administrative, and labour, in a court and before a tribunal, board or commission.

6.2 Substantive Provisions

6.2.1 General Admissibility of Electronic Records

Section 122 of the Barbados Evidence Act makes provision for the proof of contents of a document. The Act provides that a party may adduce evidence of the contents of a document if the document in question is an article or thing on or in which information is stored in such a manner that it cannot be used by the court unless a device is used to retrieve, produce or collate it, by tendering a document that was or purports to have been produced by use of the device. The Act does not, however, contain a general admissibility rule whereby documents or records would be deemed admissible even thought they are in electronic form.

Section 3 of the Belize Act provides for general admissibility which deals with non-discrimination of electronic documents. The section provides that nothing in the rules of evidence shall be applicable so as to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

In similar fashion, section 4 of the Saint Vincent and the Grenadines Act specifies that information shall not be denied legal effect, validity or enforcement solely on the ground that it is in electronic form.

The distinction made by the Jamaica Evidence Act insofar as admissibility is concerned is two-pronged: (1) Admissibility of computer evidence constituting hearsay, and (2) Admissibility of computer evidence *not* constituting hearsay. In relation to (1), a statement contained in a document produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein *unless –*

(a) *at all material times–*

  (i) *the computer was operating properly;*

  (ii) *the computer was not subject to any mal function;*

  (iii) *there were no alterations to its mechanism or processes that might reasonably be expected to have affected the validity or accuracy of the contents of the document;*

(b) *there is no reasonable cause to believe that–*

  (i) *the accuracy or validity of the document has been adversely affected by the use of any improper process or procedure or by inadequate safeguards in the use of the computer;*

  (ii) *there was any error in the preparation of the data from which the document was produced,*

(c) the computer was properly programmed;

(d) *where two or more computers were involved in the production of the document or in the recording of the data from which the document was derived –*

  (i) *the conditions specified in paragraphs (a) to (c) are satisfied in relation to each of the computers so used; and*

  (ii) *it is established by or on behalf of the person tendering the document in evidence that the use of more than one computer did not introduce any factor that might reasonably be expected to* have *had any adverse effect on the validity or accuracy of the document.*

In relation to (2), where a statement contained in a document produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in (1) above are satisfied in relation to the document.

The Trinidad and Tobago Act makes a distinction between the admissibility of computer records in civil and criminal proceedings. Section 40 of the Act deals with the admissibility of statements produced by computers and provides that in any *civil proceedings* a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown that the conditions mentioned in subsection (2) are satisfied in relation to the statement and the computer in question. The conditions outlined in subsection (2) are as follows:

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

The conditions are stated conjunctively with the result that they must all be present in order for the statements to be admissible as evidence.

Section 14B of the Act deals with the admissibility of computer records in *criminal proceedings*. The section provides that in any criminal proceedings, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein if it is shown that:

(a) there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

(b) at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and

(c) any relevant conditions specified in Rules of Court are satisfied.

The Bahamas' Act regulates Court admissibility of electronic communications in court, as follows:

7. An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is:

(a) in electronic form; or

(b) not contained in the electronic coomunication purporting to give rise to such legal effect, but is referred to in that electronic communication.

As one can see, The Bahamas' Act sets forth general admissibility for electronic communications, prohibiting discrimination solely on the basis of it being electronic or of it being referred to in a communication which is electronic.

Recommendations:

A vital component of any Electronic Evidence legislation is the provision which declares the admissibility of electronic or computer records. The differing approaches by each State derive largely from the fact that, with the exception of Belize, the relevant admissibility provision was found or was included in existing Evidence legislation. Once the central principle which provides for the admissibility of electronic or computer records or documents in civil (including administrative) and criminal proceedings is present, the form of the provision may vary, yet with the same effect being achieved. The reference to existing commonly accepted international technical or procedural standards may be of help to build presumptions on the integrity of an electronic evidence. The admissibility of electronic means for production of evidence, such as in the case of electronic videoconferencing for the hearing of accused parties or of witnesses, shall be regulated in order to avoid doubts on its legality.

6.2.2 Application of the "Best Evidence Rule"

The "best evidence rule" which is established by the common law essentially provides that where a document is adduced as substantive evidence of its contents, the original document (as opposed to a copy or any secondary evidence of its contents) is required. Due to the nature of electronic documents or records, which are difficult to class as original due to the fact that they are easily replicated and manipulated, the rule requires modification so that the best evidence rule could be satisfied upon proof of the *integrity of the electronic record systems*. This means that one must not look to the document itself but rather to the integrity of the system which produced the document for satisfaction of the "best evidence rule".

This modification is not required in the case of Barbados since the best evidence rule is abolished in the Evidence Act as follows: "The principles and rules of the common law that relate to the mode of proof of the contents of documents are abolished."

Section 6 of the Belize Act deals with the application of the best evidence rule and establishes the test of the "integrity of the electronic records system". Section 6 provides that in any legal proceedings (criminal and civil) where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied on proof of the *integrity of the electronic records system* in or by which the data was recorded or stored.

Section 6 further provides that in any legal proceedings, where an electronic record in the form of a printout has been consistently acted on, relied on or used as the actual record of the information recorded or stored on the printout, then the printout is the record for the purpose of the best evidence rule. This section indicates that once a document emanates from an electronic source, it may be considered as an electronic record even though it is in hard copy.

Recommendations:

The changeable nature of electronic records and documents without the usual trace marks as would be found in traditional documents dictates that the focus must necessarily shift from the document itself to the integrity of the *electronic records system* from which the document originates. Legislation dealing with the admissibility of electronic records or documents should therefore modify the best evidence rule to include a test for the integrity of the electronic records system. Reference to the principles of functional equivalence, precaution, and accreditation, may help apply specific rules in face of different circumstances, by providing broad commandments.

6.2.3 Authentication and the Presumption of Integrity

Authentication:

The Evidence Act of Belize provides in section 5 in relation to authentication that the person seeking to introduce the electronic record in any legal proceedings has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Section 40 of the Trinidad and Tobago Evidence Act speaks to admissibility of statements produced by computers and section 41(1) makes provision supplementary to section 40 by providing that where in any civil proceedings a statement contained in a document is proposed to be given in evidence by virtue of section 37, 39 or 40 it may, subject to any Rules of Court, be proved by the production of that document or (whether or not that document is still in existence) by the production of a copy of that document, or of the material part thereof, authenticated in such manner as the Court may approve.

In the Bahamas Act, there is determination that electronic documents shall be accepted before Courts in spite of the type of electronic authentication selected by a party, as follows:

Section 5, (2) A transaction which has been conducted using electronic means shall not be denied legal effect, validity, or enforceability because of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

Presumption of Integrity:

Despite the provision relating to authentication, section 7 of the Belize Act makes provision for the presumption of integrity of an electronic document. The rule is that in legal proceedings, there is a presumption of integrity of the electronic records system in which an electronic record is recorded or stored where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly. If the computer system was not operating properly or was out of operation, the presumption remains if the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record. Therefore, a condition precedent to the presumption arising would be that the person intending to adduce the evidence is able to prove that at all material times the computer system was operating properly or where if the computer system was not operating properly, the integrity of the record was not affected and no other reasonable grounds exist to doubt its integrity.

In Belize, the presumption also obtains where it is established that the electronic record is recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it. Further, the presumption operates where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a party who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

The Barbados' Act also makes provision for evidence produced by machines, devices, and processes etc. The terms “machines” and “processes” are not defined in the Act. The provision stipulates that where it is reasonably open to find the device or process is one that if properly used, ordinarily does what the party tendering the document asserts it to have done, it shall be presumed (unless the contrary is proved) that in producing the document on the occasion in question, the device or process did what the party asserts it to have done. The Act also deals with documents that were, at the time they were produced, part of the records of a business, whether or not the business is still in existence. Where the device or process is or was at the time used for the purposes of the business, it shall be presumed, unless the contrary is proved, that on the occasion in question the device or process did what the party adducing the evidence asserts it to have done. The foregoing section does not, however, apply in relation to the contents of a document that was produced *for the purposes of (or for purposes which included)* legal or administrative proceedings.

The Jamaica Act does not per se state that a presumption arises, but it does provide that a statement contained in a document produced by a computer shall not be admissible in any proceedings as evidence of any fact stated therein unless certain conditions are satisfied. Even though the section does not directly or expressly speak to the integrity of the computer, the conditions specified are in fact directed at proving that the computer producing the evidence has integrity. Conditions include the fact that at all material times, (i) the computer was operating properly; (ii) the computer was not subject to any mal function; and (iii) there were no alterations to its mechanism or processes that might reasonably be *ex*pected to have affected the validity or accuracy of the contents of the document. Further, a condition which must be met is that there are no reasonable grounds to believe that (i) the accuracy or validity of the document has *been* adversely affected by the use *of* any improper process or procedure or by inadequate safeguards in the use of the computer; and (ii) there was any error in the preparation *of* the data from which the document was produced. It must also be shown that the computer was properly programmed.

The Trinidad and Tobago provision is similar to that found in Jamaica in that the sections speak generally to admissibility in civil and criminal proceedings of a statement contained in a document produced by a computer upon certain conditions being met.

The Bahamas has adopted, in Section 15, § 3 of its Act, presumption of integrity of electronic networks, by establishing that "Where the received acknowledgement states that the related electronic communication met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met".

Recommendations:

Authentication and the Presumption of Integrity are vital provisions in any electronic evidence legislation. These provisions ensure that electronic evidence is admissible on proof of certain standardized criteria relating to the computer system from which evidentiary material originates. It is therefore recommended that these provisions should be included in electronic evidence or evidence legislation. Computer forensics shall be employed in technical discovery proceedings where necessary to make proof of the existing digital environment at the time of the facts submitted to Court appraisal.

6.2.4 Standards, Proof of Affidavit and Cross Examination

Section 8 of the Belize Act deals with Standards and specifies that where one seeks to determine under any rule of law whether electronic evidence is admissible, evidence may be presented of any standard, procedure, usage or practice on how electronic records are to be recorded and preserved having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Section 9 of the Belize Act provides that the matters set out in the sections dealing with the application of the best evidence rule (section 6), the presumption of integrity (section 7) and standards (section 8) may be established by an affidavit given to the best of the deponents knowledge and belief. Section 10 provides that the deponent of an affidavit introduced in evidence under section 9 may be cross-examined as of right by a party to proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

The provision in the Jamaica Evidence Act which deals with the admissibility of computer evidence constituting hearsay provides for the person tendering the document in evidence to establish that the use of more than one computer did not introduce any factor that might reasonably be expected to have had any adverse effect on the validity or accuracy of the document. Such proof may include facts relating to the integrity of the system and the standards and procedures used in the preservation of records.

The Trinidad and Tobago Act provides for certificates to be issued in respect of statements desired to be used as evidence in civil and criminal proceedings which are derived from a computer. The certificate *(a)* identifying the document containing the statement and describing the manner in which it was produced; *(b)* giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer; *(c)* dealing with any of the matters mentioned in subsection (1-criminal) or (2-civil) relate [admissibility]; and *(d)* signed by a person occupying a responsible position in relation to the operation of the computer, shall be evidence of anything stated in such certificate, and the Act states that it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it. Despite the ability to produce such a certificate, a court may require oral evidence to be given of anything of which evidence could be given by a certificate. Any person who in a certificate tendered makes a statement which that person knows to be false or does not believe to be true is guilty of an offence and liable on conviction to a fine or imprisonment.

Recommendations:

Electronic Evidence legislation should provide a mechanism by which conditions to be complied with in relation to standards, the presumption of integrity, the best evidence rule and other related issues may be proved by the submission of an affidavit deposing to the relevant facts. The deponent of an affidavit should be cross-examined as of right by the party to the proceedings who is adverse in interest to the party adducing the affidavit. These provisions are necessarily a direct result and response to the nature of electronic evidence which may be manipulated. It is also necessary to ensure as far as possible that the evidence being adduced was retrieved from a system which has integrity. Search and seizure proceedings shall be regulated in a way to avoid that the collection of evidence be questioned as not having certified and produced material evidence of the data collected and of the existing digital environment. The principle of no compulsory self-incrimination shall be respected.

6.2.5 Agreement on Admissibility of Electronic Records

It is only the Belize provision which allows agreement on the admissibility of electronic records between the parties. Section 11 of the Act allows the parties to civil and criminal proceedings to expressly agree at any time that its admissibility may not be disputed. However, an agreement between the parties on admissibility of electronic records does not render the record admissible in criminal proceedings on behalf of the prosecution if at the time the agreement was made, the accused was not represented by an Attorney-at-Law.

Recommendations:

The agreement on admissibility of electronic records is a useful provision for purposes of adducing electronic evidence with expedition in legal proceedings and doing so in a more cooperative fashion to cut costs for litigants. Extension to criminal proceedings may be subject to constraints.

6.2.6 Admissibility of Electronic Signature

Section 11 of the Belize Act deals with the admissibility of electronic signatures. It provides that where a rule of evidence requires a signature or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences. Further, an electronic signature may be proved in any manner such as by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic signature is that of the person.

Section VI

The Saint Vincent and the Grenadines Act also contains provisions for electronic signatures. Section 22 of the Act states that if a rule of law requires the signature of a person, the requirement is met by an electronic signature if the electronic signature that is used is as reliable and as appropriate for the purpose for which it was generated or communicated. If a rule of law provides consequences for the absence of a signature, those consequences are avoided with the use of an electronic signature. The provision also states that an electronic signature is not without legal force and effect merely on the ground that it is in electronic form. Parties are at liberty to agree to use a particular method of electronic signature, unless otherwise provided by law. A person relying on an electronic signature shall bear the legal consequences of his failure to take reasonable steps to verify the reliability of an electronic signature. In determining whether or to what extent information in electronic form is legally effective, no regard shall be had to the location where the information was created or used or to the place of business of its creation.

It is notable that while both Belize and Saint Vincent and the Grenadines have included a provision on electronic signature in their respective Acts, the provisions differ in terms of complexity. For Belize, the parties are at liberty to agree on the type of signature to be used between them. While this can also be done in Saint Vincent and the Grenadines, the Act also creates an Accreditation Authority to accredit authentication products or services which are designed to identify the holder of an electronic signature to other persons. The Authentication Authority may not accredit authentication products or services unless the Authority is satisfied that an electronic signature to which such authentication products or services relate (a) is uniquely linked to the user, (b) is capable of identifying the user, (c) is created using means that can be maintained under the sole control of the user, (d) will be linked to the information to which it relates in such a manner that any subsequent change of the information is detectable; and (e) is based on the face to face identification of the user.

Electronic signature is acceptable in The Bahamas in the following terms:

9.(1) Where the law requires the signature of a person, that requirement is met in relation to an electronic communication if a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic communication.

Recommendations:

The insertion of provisions in relation to electronic signatures is crucial to the implementation of an Electronic Evidence law as it may achieve the functional equivalence between electronic and paper documents which is necessary for the recognition and legal enforcement of electronic records. It is therefore recommended that a provision for electronic signatures be inserted in legislation whether in a separate Electronic Evidence Act, in existing Evidence legislation or Electronic Transactions or Electronic Commerce legislation. For small jurisdictions, it may be costly and resource intensive to establish an Accreditation Authority in terms of the Saint Vincent and the Grenadines model. The Belize model is therefore recommended for ease of implementation and the minimal or no costs attached for either the user or the State. Given the importance of properly dating electronic documents, thus enabling them to serve as evidence of the time of an act or document and to better allow for search of stored data, the certifying authority shall be empowered and required to also certify the time of electronic records ("time-stamping"). The implementation of digital signature with certification of attributes constitutes additional evidence (including, for implementation of electronic judicial proceedings).

Section VII: Assessment of Regional Texts

7.1 Overview of Assessment Ratings

The following countries do not have Electronic Evidence legislation or Evidence legislation containing electronic evidence provisions enacted: Antigua and Barbuda, Dominica, Dominican Republic, Grenada, Guyana, Haiti, St. Kitt & Nevis, Saint Lucia, Suriname.

Key

GOOD: There is legislation adequately which addresses the key issues.

FAIR: There is some form of reference to the issues in legislation which does not adequately address the key issues.

LIMITED: There is reference on the form of policy or consultation document or draft legislation.

NONE: There is no reference in the legislative texts to the key issues.

Country/Region	Definitions (computer, Document and legal proceedings)	General admissibility of electronic records	Application of the best evidence rule	Authentication	Presumption of integrity	Standards, Proof of affidavit and cross examination	Agreement of admissibility of electronic records	Admissibility of electronic signature
Antigua and Barbuda	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
The Bahamas	LIMITED	GOOD	NONE	GOOD	GOOD	NONE	NONE	GOOD
Barbados	FAIR	LIMITED	NONE	NONE	GOOD	NONE	NONE	GOOD
Belize	FAIR	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	NONE
Dominica	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Dominican Republic	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Grenada	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Guyana	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	LIMITED	GOOD	NONE	NONE	FAIR	GOOD	NONE	NONE
St. Kitts and Nevis	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Saint Lucia	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
St. Vincent and the Grenadines	NONE	GOOD	NONE	NONE	NONE	NONE	NONE	GOOD
Suriname	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago	FAIR	GOOD	NONE	GOOD	FAIR	GOOD	NONE	NONE

7.2 Matrix of Legal Provisions

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
Legal Provisions:					
Definitions:					
"computer"					
"data"		**"data"** means representations, in any form, of information or concepts			
"document" or "electronic record"	**"document"** includes (a) anything on which there is writing; (b) a map, plan, drawing or photograph; and (c) any information recorded or stored by means of any tape recorder, computer or other device, and any material subsequently derived from the information so recorded or stored;	**"electronic record"** means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device and includes a display, print out or other output of that data;	**"Document"** 31B. In this Part– **"document"** includes, in addition to a document in s.3, *(a)* any map, plan, graph or drawing; *(b)* any photograph; *(c)* any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied *so* as *to* be capable (with or without the aid of some other equipment) of being reproduced therefrom;		**"record"** means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;
			(d) any film (including microfilm), negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom.		

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
"electronic records system"		**"electronic records system"** includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records;			
"legal proceedings"	**"legal or administrative proceedings"** means proceedings, however described; *(a)* in a court in Barbados or a court of a foreign country; or	**"legal proceedings"** means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.			
	(b) before a person or body, other than a court, authorised by law, including a law of a foreign country, or by consent of parties, to hear and receive evidence, and includes proceedings in a coroner's court and proceedings in a court martial; **"civil proceedings"** means proceedings in a court, other than criminal proceedings; **"criminal proceedings"** means a prosecution in a court for an offence, and includes proceedings for the commitment of a person for trial for an offence;				

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
General admissibility of electronic records	**Proof of contents of documents.** **122. (1)** A party may adduce evidence of the contents of a document in question – *(a)* by tendering the document in question;	**General admissibility.** 3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.	**Admissibility of computer evidence constituting hearsay.** 31G. A statement contained in a document produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein unless–	**Non-discrimination against electronic information.** 4. (1) Information shall not be denied legal effect, validity or enforcement solely on the ground that it is in electronic form.	**General admissibility.** 7. An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is: a) in electronic form; or
	(b) by adducing evidence of an admission made by some other party to the proceeding as to the contents of the document in question; (c) by tendering a document that (i) is or purports to be a copy of the document in question, and (ii) has been produced, or purports to have been produced, by a device that reproduces the contents of documents; (d) if the document in question is an article or thing by which words are recorded in such a way as to be capable of being reproduced as sound, or in which words are recorded in a code, including shorthand writing, by tendering a document that is or purports to be a transcript		(a) at all material times- (i) the computer was operating properly; (ii) the computer was not subject to any mal function; (iii) there was no alterations to its mechanism or processes that might reasonably be *ex*pected to have affected the validity or accuracy of the contents of the document; (b) there is no reasonable cause to believe that – (i) the accuracy or validity of the document has *been* adversely affected by the use *of* any improper process or procedure or by inadequate safeguards in the use of the computer; (ii) there was any error in the preparation *of* the data from which the document was produced,	**(2)** In sections 5, 6, 7, 8 and 22: (a) where a rule of law require information to be in writing, given, signed, original or retained, the requirement is met if the section is complied with; (b) where a rule of law provides consequences where the information is not in writing, given, signed, original or retained, the consequences are avoided if the section is complied with; and (c) where a rule of law provides consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.	b) not contained in the electronic coomunication purporting to give rise to such legal effect, but is referred to in that electronic communication.

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
	of the words;		(c) the computer was properly programmed;		
	(e) if the document in question is an article or thing on or in which information is stored in such a manner that it cannot be used by the court unless a device is used to retrieve, produce or collate it, by tendering a document that was or purports to have been produced by use of the device; (f) by tendering a document that (i) forms part of the records of or kept by a business whether or not the business is still in existence, and (ii) purports to be a copy of, or an extract from or a summary of, the document in question, or is or purports to be a copy of such a document; or (g) if the document in question is a public document, by tendering a document, that was or purports to have been printed– (i) by the Government Printer, or		*(d)* where two or more computers were involved in the production of the document or in the recording *of the* data from which the document was derived – (i) the conditions specified in paragraphs *(a)* to *(c)* are satisfied in relation to each of the computers *so* used; and (ii) it is established by or on behalf *of* the person tendering the document in evidence *that* the use of more than one computer did not introduce any factor that might reasonably be expected to have had any adverse effect on the validity or accuracy of the document.	**Evidence.** **83.** In proceedings for an offence against a law of Saint Vincent and the Grenadines, the fact that: (a) it is alleged that an offence of interfering with an information system has been committed; and (b) evidence has been generated from that information system; does not of itself prevent that evidence from being admitted.	

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
	(ii) by the authority of the government of a foreign country, and is or purports to be a copy of the document in question. (2) Subsection (1) applies in relation to a document in question, whether the document in question is available to the party or not. (3) A party may adduce evidence of the contents of a document in question that is unavailable – (a) by tendering a document that is a copy of, or a faithful extract from or summary of, the document in question; or (b) by adducing oral evidence of the contents of the document in question.		**Admissibility of computer evidence not constituting hearsay.** 31H. Where a statement contained in a document produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in section 31G are satisfied in relation to that document.		
	Documents in foreign countries. **123.** Where the document in question is in a foreign country, paragraph *(b),* (c), *(d),* (e) or (f) of subsection (1) of section 122 does not apply unless – *(a)* the party who adduces evidence of the contents of the document in question has, not less than 14 days before the day on which the evidence is adduced, served				

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
	on each other party a copy of the document proposed to be tendered; or *(b)* the court directs that it is to apply.				
Scope of Act		**Scope of Act.** 4. (1) This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.			
		(2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.			
Authentication		**Authentication.** 5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.			**Authentication.** Section 5, (2) A transaction which has been conducted using electronic means shall not be denied legal effect, validity, or enforceability because of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
Application of best evidence rule	**Best evidence rule abolished.** 121. The principles and rules of the common law that relate to the mode of proof of the contents of documents are abolished.	**Application of best evidence rule.** 6. (1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.			
		(2) In any legal proceeding, where an electronic record in the form of a printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purpose of the best evidence rule.			
Presumption of integrity	**Evidence produced by machines, processes, etc.** 124. (1) This section applies in relation to a document or thing produced wholly or partly by a device or process.	**Presumption of integrity.** 7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:	**Admissibility of computer evidence constituting hearsay.** 31G. A statement contained in a document produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein unless –		**Presumprion of integrity** Section 15, § 3, Where the received acknowledgement states that the related electronic communication met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
			(a) at all material times- (i) the computer was operating properly; (ii) the computer was not subject to any mal function;		
	(2) Where it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily does what the party tendering the document or thing asserts it to have done, it shall be presumed, unless the contrary is proved, that, in producing the document or thing on the occasion in question, the device or process did what that party asserts it to have done. (3) In the case of a document that is, or was at the time it was produced, part of the records of, or kept for the purposes of, a business, whether or not the business is still in existence, then where the device or process is or was at that time used for the purposes of the business, it shall be presumed, unless the contrary is proved, that on the occasion in question the device or process did what	*(a)* where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record; *(b)* where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or	(iii) there was no alterations to its mechanism or processes that might reasonably be *ex*pected to have affected the validity or accuracy of the contents of the document; (b) there is no reasonable cause to believe that – (i) the accuracy or validity of the document has *been* adversely affected by the use *of* any improper process or procedure or by inadequate safeguards in the use of the computer; (ii) there was any error in the preparation *of* the data from which the document was produced, (c) the computer was properly programmed; *(d)* where two or more computers were involved in the production of the document or in the recording *of the* data from which the document was derived –		

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
	the party adducing the evidence asserts it to have done.		(i) the conditions specified in paragraphs *(a)* to *(c)* are satisfied in relation to each of the computers *so* used; and		
	(4) Subsection (3) does not apply in relation to the contents of a document that was produced for the purposes of, or for purposes that included the purposes of, legal or administrative proceedings.	*(c)* where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.	*(c)* are satisfied in relation to each of the computers so used; and (ii) it is established by or on behalf *of* the person tendering the document in evidence *that* the use of more than one computer did not introduce any factor that might reasonably be expected to have had any adverse effect on the validity or accuracy of the document. **Admissibility of computer evidence not constituting hearsay.** 31H. Where a statement contained in a document produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in section 31G are satisfied in relation to that document.		
Standards		**Standards.** 8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may			

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
		be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.			
Proof of affidavit		**Proof of affidavit.** 9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.			
Cross-examination		**Cross-examination.** 10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced. (2) Any party to the proceedings may, with leave of the court, cross-			

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
		examine a person referred to in paragraph *(c)* of section 7.			
Agreement on admissibility of electronic records		**Agreement on admissibility of electronic records.** 11. (1) Unless otherwise provided in any other law, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.			
		(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by an attorney-at-law.			
Admissibility of electronic signature		**Admissibility of electronic signature.** 12. (1) Where a rule of evidence requires a signature, or provides for		**Signature** 22. (1) If a rule of law requires the signature of a person, the requirement is met by an electronic	**Admissibility of electronic signature.** 9.(1) Where the law requires the signature of a person, that requirement is met in

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
		certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.		signature if the electronic signature that is used is as reliable and as appropriate for the purpose for which it was generated or communicated, in all the circumstances, including any relevant agreements.	relation to an electronic communication if a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic communication.
		(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.		**(2)** Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the rule of law provides consequences for the absence of a signature. **(3)** An electronic signature is not without legal force and effect merely on the ground that is in electronic form. **(4)** Parties may agree to use a particular method of electronic signature, unless otherwise provided by law. **(5)** Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, the requirement is met in relation to the data message if:	

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
				(a) the signature creation data is linked to the signatory and no other person;	
				(b) the signature creation data at the time of signing is under the control of the signatory and no other person; (c) any alteration to the electronic signature, made after the time of signing is detectable; and (d) where a purpose of the legal requirement for a signature is to provide assurance as to the soundness of the information to which it relates, any alteration made to that information after the time of signing is detectable. **(6)** Subsection (5) does not limit the ability of a person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an electronic signature; or (b) to adduce evidence of the non-reliability of an electronic signature.	

	Barbados	Belize	Jamaica	Saint Vincent and the Grenadines	The Bahamas
				Standards for signatures **23.** The Minister may make Regulations prescribing methods which satisfy the requirements of section 22. **Conduct of a person relying on an electronic signature** **24.** A person relying on an electronic signature shall bear the legal consequences of his failure to take reasonable steps to verify the reliability of an electronic signature. **Recognition of foreign electronic documents and signatures.** **25.** In determining whether or to what extent information in electronic form is legally effective, no regard shall be had to the location where the information was created or used or to the place of business of its creation.	

Section VIII:
Policy Guidelines

As seen in the preceding sections, the variety of issues behind legislative options regarding electronic evidence is significant, thus the importance of policy-making in deciding about such options. This section points to different issues and relevant criteria, in the aim of helping to guide policy-making.

8.1 Terminology

Although some laws (most of them, at least five years old now) contain a glossary providing definition on terms such as "computer", "computer data", and others, technological progress has apportioned new features and functions (for instance, technologies convergence, merging informatics and telecommunications) indicate that some definitions shall be reviewed or updated, as to their scope and language.

Definitions shall neither be too much specific, otherwise they may become prematurely obsolete, nor too generic. Conceptual wording, plus some illustrative examples, seems to be a more balanced solution.

How much to be left for judicial construction on definitions is another option to be thought about, as there are experiences where Courts have been able to fix terminology problems[6].

8.2 Time-Stamping

Although the authorship, authenticity and integrity of electronic documents are more popularly associated with digital signatures, time is of the essence in several acts, deeds, and contracts, so the convenience of adoption of "time-stamping" (certification of time) is equally important, also because "time-stamping" is an additional way to evidence integrity of an electronic file, and it provides proper criterion for searches in databases (for instance, the search of an e-mail message within the messages that flow through major ISPs in a day involve massive quantities of data, and the clock either of the sender, of the addressee, or of the ISP may have different times, what makes it usually impossible to comply with Court orders to find and seize some e-mail message.

8.3 Procedural Standards

Digital signatures have been considered a secure way of evidencing authorship, authenticity and integrity of electronic evidence, especially where advanced technology and certification are involved. However, the widespread use of botnets have transformed the notions of an equipment associated with certain user, as a "zombie" computer may be used by someone else, inclusively making use of the digital signature of the owner of the computer.

---

[6] "After hearing the evidence in this case the first finding the court is constrained to make is that, in the computer age, lawyers and courts need no longer feel ashamed or even sensitive about the charge, often made, that they confuse the issue by resort to legal "jargon", law Latin or Norman French. By comparison, the misnomers and industrial shorthand of the computer would make the most esoteric legal writing seem as clear and lucid as the Ten Commandments or the Gettysburg Address; and to add to this Babel, the experts in the computer field, while using exactly the same words, uniformly disagree as to precisely what they mean. Such being the state of the art, the court concludes that before even discussing the contract it should make at least a preliminary attempt at computer definitions." Edenfield, J. Honeywell, Inc. v. Lithonia Lighting, Inc., 317 F. Supp. 406, 408, 2 CLSR 894, 896 (N.D. Ga. 1980), quoted in Computer Law Association's "Computer Terminology – Judicial and Administrative Definitions", Robert P. Bigelow, Esq. (1993 revisions by Esther C. Roditti).

Several threats exist nowadays that make the security of a computer a question mark. International and national technical standards associations have issued procedural norms which may serve as guidance for defining which tests a computer shall go through to confirm its integrity. Some international treaties and conventions and some national laws have opted to nominate the standards organizations which norms shall be considered as parameters for meeting law requirements.

8.4 Criptography

Encryption technologies may be a defense, or a threat. For instance, electronic judicial proceedings which run under secrecy of Justice may be encrypted, to ensure confidentiality. However, encryption has been used also for illicit purposes, such as money-laundering, and terrorism, and may turn impossible to reveal the contents of protected electronic files. The easy and inexpensive access to encryption technologies suggests that regulation of electronic evidence shall already focus on this issue.

Therefore, a close connection must be established with laws on interception of communications and on digital signature, to make sure that proactive and/or reactive cooperation from ISPs and from technology providers can be required.

8.5 Images

In a time of increasingly "visual" culture, the quantity of documents made of images tends to, progressively, rival the volume of "text" documents. Hence, it does not seem to be the case (at least, presently) to exclude images from the definition of "document", as it has been done in some national laws.

The inclusion of images within the concept of "document also has a security reason: criminals have used *steganography* to hide illicit messages behind electronic images. Thus, if electronic images are not considered as electronic documents, the investigation and repression of those cases may be compromised.

8.6 Digital Signature

Most countries have not implemented a single personal identification number for each individual, including all means of identification in a single document.

Digital signature may better identify one person or entity where certification of attribute is ensured, avoiding the use of digital signature by whom is not entitled to it. Certification of attributes such as profession, title, position in an organization, and others, is capable of enhancing the evidential power of digital signature.

8.7 Videoconferencing

Integration of informatics and telecommunications is now a reality, represented by smart phones, digital tv, and other examples.

"Electronic" evidence has become also "telecommunications" evidence, much beyond traditional phone conversation recording.

This has to do not only with definitions and terminology but also with methods of producing evidence, such as oral evidence. The difficulty or cost of transporting accused parties or witnesses for depositions, while electronic videoconferencing is now accompanied of voice-over-IP secure technologies and of filming possibilities with cameras placed in different angles and shown simultaneously, has motivated the updating of legislation in some countries. This may also be of interest for situations of regional, Community integration of Justice.

ANNEXES

Annex 1: Bibliography

"Computer Terminology – Judicial and Administrative Definitions", Robert P. Bigelow, Esq., Computer Law Association, 1993 revisions by Esther C. Roditti.

Joly-Passant, Elisabeth, "L'Écrit Confronté aux Nouvelles Technologies", Paris, L.G.D.J., 2006. Rimbaud, Alexis, "Le Juge Pénal et l'Expertise Numérique", Paris, Dalloz, 2007.

Bensoussan, Alain, and Le Roux, Yves, "Cryptologie et signature életronique – aspects juridiques", Paris, Hermes, 1999.

Marcacini, Augusto Tavares Rosa, "Direito e informática – uma abordagem jurídica sobre criptografia", Rio de Janeiro, Forense, 2002.

Capriolli, Eric A., "Droit international de l'économie numérique", Paris, Litec, 2007.

Santolim, César Viterbo Matos Santolim, "Formação e Eficácia Probatória dos Contratos por Computador", São Paulo, Saraiva, 1995.

Márquez, José Fernando, "Firma Digital Argentina", Buenos Aires, LexisNexis Abeledo-Perrot, 2002.

Volpi, Marlon Macedo, "Assinatura Digital – aspectos técnicos, práticos e legais", Rio de Janeiro, Axcel, 2001.

Clara, Bibiana Luz, "Ley de Firma Digital Comentada", Rosario, Nova Tesis, 2006. Carvalho, Paulo Roberto de Lima, "Prova cibernética no processo", Curitiba, Juruá, 2009. Cachard, Olivier, "La Régulation Internationale du Marche Électronique", Paris, L.G.D.J., 2001.

"Prova Judiciária – estudos sobre o novo direito probatório", Knijnik, Danilo (coord.), Porto Alegre, do Advogado, 2007.

Chatillon, Georges, "Internet International Law", Brussels, Bruylant, 2005.

Céspedes, José Francisco Espinoza, "Contratación Electrónica, Medidas de Seguridad y Derecho Informático", Lima, Rao, 2000.

Castrillo, Eduardo de Urbano, "La valoración de la prueba electrónica", Valencia, Tirant Lo Blanch, 2009. Rinessi, Antonio Juan, "El Deber de Seguridad", Buenos Aires, Rubinzal-Culzoni, 2007.

Annex 2:

Participants of the First Consultation Workshop for HIPCAR Working Group 1, dealing with ICT Legislative Framework – Information Society Issues
Gros Islet, Saint Lucia, 8-12 March 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre

Annex 2

Country	Organization	Last Name	First Name
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatie Autoriteit Suriname / Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Project Experts

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[7]	J Paul
PRESCOD	Kwesi

[7] Workshop Chairperson

Annex 3A:

BELIZE
Chapter 95:01
ELECTRONIC EVIDENCE
[31st January, 2003]

1. This Act may be cited as the Electronic Evidence Act.

2. In this Act unless the context otherwise requires: –

"data" means representations, in any form, of information or concepts;

"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device and includes a display, print out or other output of that data;

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records;

"legal proceedings" means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

4. (1) This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

(2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

6. (1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of a printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purpose of the best evidence rule.

7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record;

(*b*) where it is established that the electronic record was recorded or stored by a party to the proceedings Who is adverse in interest to the party seeking to introduce it; or

(c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.

10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in paragraph (c) of section 7.

11. (1) Unless otherwise provided in any other law, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by an attorney-at-law.

12. (1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

Annex 3B:

JAMAICA Chapter 7:02
EVIDENCE ACT

An Act Relating to the Law of Evidence.

[14th September 1905]
[15th June 1855] [22nd June 1898]

1. This Act may be cited as the Evidence Act.

PART I
GENERAL

2. Whenever any question arises in any action, suit, information, or other proceeding in or before any Court of Justice, or before any person having by law or by consent of parties authority to hear, receive, and examine evidence touching the admissibility or the sufficiency of any evidence, or the competency or obligation of any witness to give evidence, or the swearing of any witness, or the form of oath or of affirmation to be used by any witness, or the admissibility of any question put to any witness, or the admissibility or sufficiency of any document, writing, matter, or thing tendered in evidence, every such question shall be decided according to the law in force in England on 30th August 1962.

3 A Court shall take judicial notice of any statutory instrument made under a written law of Trinidad and Tobago if the statutory instrument has been published in the Gazette or in the Revised Edition of the Laws of Trinidad and Tobago.

4. The written laws of the legislature of any Commonwealth territory may be proved by copies thereof purporting to be printed by the authority of the legislature or the Government of that country.

5. A party producing a witness shall not be allowed to impeach his credit by general evidence of bad character, but he may, in case the witness in the opinion of the Judge proves adverse, contradict him by other evidence, or by leave of the Judge, prove that he had made at other times a statement inconsistent with his present testimony; but before such last-mentioned proof can be given, the circumstances of the supposed statement, sufficient to designate the particular occasion, must be mentioned to the witness, and he must be asked whether or not he has made such statement.

6. If a witness, upon cross-examination as to a former statement made by him relative to the subject matter of the indictment or proceeding and inconsistent with his present testimony, does not distinctly admit that he did make the statement, proof may be given that he did in fact make it; but before such proof is given, the circumstances of the supposed statement, sufficient to designate the particular occasion, shall be mentioned to the witness, and he shall be asked whether or not he made the statement.

7. A witness may be cross-examined as to previous statements made by him in writing, or reduced into writing, relative to the subject matter of the indictment or proceeding without the writing being shown to him; but if it is intended to contradict the witness by the writing, his attention must, before such contradictory proof is given, be called to those parts of the writing which are to be used for the purpose of so contradicting him; but the Judge, at any time during the trial, may require the production of the writing for his inspection, and may make such use of it for the purposes of the trial as he thinks fit.

8. A witness may be questioned as to whether he has been convicted of any indictable offence, and upon being so questioned, if he either denies or does not admit the fact, or refuses to answer, the cross-examining party may prove the conviction; and a certificate containing the substance and effect only (omitting the formal part) of the indictment and conviction for such offence, purporting to be signed by the Registrar or Clerk of the Court, or other officer having the custody of the records of the Court where the offender was convicted, or by the deputy of such Clerk or officer, is, upon proof of the identity of the person, sufficient evidence of the conviction, without proof of the signature or official character of the person appearing to have signed the same.

9. It is not necessary to prove by the attesting witness any instrument to the validity of which attestation is not requisite, and the instrument may be proved as if there had been no attesting witness.

10. Comparison of a disputed writing with any writing proved to the satisfaction of the Judge to be genuine is permitted to be made by witnesses; and such writing, and the evidence of witnesses respecting it, may be submitted to the Court and jury as evidence of the genuineness or otherwise of the writing in dispute.

11. This Part shall apply to all Courts of Justice, criminal as well as all others, and to all persons having, by law or by consent of parties, authority to hear, receive, and examine evidence.

12. ***(Repealed by Act No. 28 of 1996).***

PART II
EVIDENCE IN CRIMINAL CASES

13. (1) Every person charged is a competent witness for the defence at every stage of the proceedings, whether the person so charged is charged solely or jointly with any other person; but –

(a) a person so charged shall not be called as a witness in pursuance of this section except upon his own application;

(b) the failure of any person charged with an offence, to give evidence shall not be made the subject of any comment by the prosecution;

(c) ***(Repealed by Act No. 28 of 1996).***

(2) A person charged and being a witness in pursuance of this section may be asked any question in cross-examination, notwithstanding that it would tend to criminate him, as to the offence charged.

(3) A person charged and called as a witness in pursuance of this section shall not be asked, and if asked shall not be required to answer, any question tending to show that he has committed or been convicted of or been charged with any offence other than that wherewith he is then charged, or is of bad character, unless –

(a) the proof that he has committed or been convicted of such other offence is admissible evidence to show that he is guilty of the offence wherewith he is then charged; or

(b) he has personally or by his advocate asked questions of the witnesses for the prosecution with a view to establish his own good character, or has given evidence of his good character, or the nature or conduct of the defence is such as to involve imputations on the character of the prosecutor or the witnesses for the prosecution or the victim who is deceased or otherwise incapable of giving evidence of the alleged crime; or

(c) he has given evidence against any other person charged with the same offence.

(4) A person called as a witness in pursuance of this section shall, unless otherwise ordered by the Court, give his evidence from the witness box or other place from which the other witnesses give their evidence.

(5)

(6)

13A. (1) Subject to this Act and the Children Act, every person is competent and compellable to give evidence.

(2) A person who is incapable of understanding that he is under an obligation to give truthful evidence is not competent to give evidence.

(3) Where in the opinion of the Court a person is incapable of understanding and of communicating a reply to a question and where that incapacity cannot be readily overcome for the purposes of the trial, that person is deemed incompetent to give evidence.

13B. (1) Subject to subsections (2) and (3), where a person is charged on indictment, he shall not be entitled to make a statement without being sworn, and accordingly if he gives evidence he shall do so on oath and be liable to cross-examination.

(2) Nothing in subsection (1) shall–

(a) affect the right of a person charged, if not represented by an Attorney-at-law, to address the Court or jury otherwise than on oath on any matter on which, if he were so represented, such attorney-at-law could address the Court or jury on his behalf; or

(b) prevent him from making a statement without being sworn, if–

(i) the statement is one which he is by law required to make personally; or

(ii) the statement is made by way of mitigation before the Court passes sentence upon him.

(3) Nothing in this section shall apply to a trial which began before the commencement of this section.

14. (1) In this section–

“statement” includes any representation of fact, whether made in words or otherwise; “document” includes any device by means of which information is recorded or stored; and

“business” includes every kind of business, profession, occupation, calling, operation or activity, whether carried on for profit or otherwise.

(2) In any criminal proceeding where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, on production of the document, be admissible as evidence of that fact if–

(a) the document is, or forms part of, a record relating to any trade or business and compiled, in the course of that trade or business, from information supplied (whether directly or indirectly) by persons who have, or may reasonably be supposed to have, personal knowledge of the matters dealt with in the information they supply; and

(b) the person who supplied the information recorded in the statement in question is dead, or beyond the seas, or unfit by reason of his bodily or mental condition to attend as a witness, or cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which has elapsed since he supplied the information and to all the circumstances) to have any recollection of the matters dealt with in the information he supplied.

(3) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of this section, the Court may draw any reasonable inference from the form or content of the document in which the statement is contained, and may, in deciding whether or not a person is fit to attend as a witness, act on a certificate purporting to be a certificate of a registered medical practitioner.

(4) In determining the weight, if any, to be attached to a statement admissible as evidence by virtue of this section regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement, and, in particular, to the question whether or not the person who supplied the information recorded in the statement did so contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not that person, or any person concerned with making or keeping the record containing the statement, had any incentive to conceal or misrepresent the facts.

(5) Nothing in this section affects the admissibility of any evidence that would be admissible apart from this section, or makes admissible any statement or document that is privileged.

14A. (1) Subject to subsection (2), in any criminal proceedings a photograph of any object may be admitted in evidence as prima facie proof of the identity of that object, provided that the photograph is supported by a certificate signed by the photographer before a Justice of the Peace authenticating the photograph as being a true image of the object aforesaid.

(2) The photographer shall be required to give evidence of the procedure adopted by him to produce the photograph.

14B. (1) In any criminal proceedings, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein if it is shown that–

(a) there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

(b) at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and

(c) any relevant conditions specified in Rules of Court are satisfied.

(2) Provision may be made by Rules of Court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section, such information concerning the statement as may be required by the Rules shall be provided in such form and at such times as may be so required.

(3) In any proceedings where it is desired to give a statement in evidence in accordance with subsection (1), a certificate–

(a) identifying the document containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

(c) dealing with any of the matters mentioned in subsection (1); and

(d) signed by a person occupying a responsible position in relation to the operation of the computer,

shall be evidence of anything stated in such certificate, and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(4) Notwithstanding subsection (3), a Court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.

(5) Any person who in a certificate tendered under subsection (3), makes a statement which he knows to be false or does not believe to be true is guilty of an offence and liable–

(a) on summary conviction to a fine of three thousand dollars and to imprisonment for six months;

(b) on conviction on indictment to a fine of ten thousand dollars and to imprisonment for two years.

(6) In estimating the weight, if any, to be attached to a statement admitted pursuant to this section regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular–

(a) to the question whether or not the information reproduced in or derived from the statement was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

(b) to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced, had any incentive to conceal or misrepresent the facts.

(7) For the purposes of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or, with or without human intervention, by means of any appropriate equipment.

(8) For the purpose of deciding whether or not a document is admissible in evidence by virtue of subsection (1) the Court may draw any reasonable inference–

(a) from the circumstances in which the statement was made or otherwise came into being; or

(b) from any other circumstance, including the form and contents of the document in which the statement is contained.

14C. Where a statement contained in a document is admissible in criminal proceedings, it may be proved–

(a) by the production of that document; or

(b) by the production of a copy of that document, or of the material part of it, whether or not that document is still in existence,

and authenticated in such manner as the Court may approve; and it is immaterial for the purposes of this section the extent to which the original or a copy thereof may have been reproduced.

14D. (1) In any criminal proceeding or inquest, any record kept by a Government expert relating to anything submitted to him for examination, analysis or report shall be prima facie evidence of the particulars recorded therein.

(2) For the purposes of subsection (1) "Government expert" has the same meaning as that expression bears in section 19(4).

14E. The Rules Committee established by the Supreme Court of Judicature Act, may, subject to negative resolution of Parliament, make Rules necessary for the purposes of this Part.

15. (1) Where the only witness to the facts of the case called by the defence is the person charged, he shall be called as a witness immediately after the close of the evidence for the prosecution.

(2) In cases where the right of reply depends upon the question whether evidence has been called for the defence, the fact that the person charged has been called as a witness shall not of itself confer on the prosecution the right of reply.

15A.(1) Any requirement at common law whereby at a trial on indictment it is obligatory for the Court to give the jury a warning about convicting the accused on the uncorroborated evidence of a person because that person is–

(a) an alleged accomplice of the accused; or

(b) a person in respect of whom it is alleged that a sexual offence under the Sexual Offences Act, has been committed,

is abrogated.

(2) Any requirement that is applicable at the summary trial of a person for an offence and corresponds to the requirement mentioned in subsection (1) is abrogated.

(3) Nothing in this section shall prevent a Judge from exercising his discretion to advise a jury of the need for corroboration.

(4) Nothing in this section applies to any trial on indictment or to any proceedings before a Magistrate's Court which began before the commencement of this section.

PART III
EVIDENCE IN PARTICULAR CASES

16. The parties to any action for breach of promise of marriage are competent to give evidence in such action; but no plaintiff in any action for breach of promise of marriage may recover a verdict unless his or her testimony is corroborated by some other material evidence in support of such promise.

17. The parties to any proceeding instituted in consequence of adultery, and their husbands and wives are competent to give evidence in such proceeding, but no witness in any proceeding, whether a party to the suit or not, shall be liable to be asked or bound to answer any question tending to show that he or she has been guilty of adultery, unless such witness has already given evidence in the same proceeding in disproof of his or her alleged adultery.

18. The parties to any information or proceeding in the High Court for the recovery of any penalty for the breach of any law relating to the revenue are competent to give evidence in any such information or proceeding.

19. (1) A document purporting to have affixed, impressed, or subscribed thereon or thereto the seal and signature of any diplomatic agent of Trinidad and Tobago in any foreign country, or any consular officer of Trinidad and Tobago in any foreign place, in testimony of any oath, affidavit, or act administered, taken, or done by or before any such person shall be admitted in evidence in any Court of Trinidad and Tobago without proof of his seal or signature or of his official character.

(1A) Where a document is attested to in a foreign country and purports to have affixed, impressed, or subscribed thereon the seal and signature of a notary public, a commissioner for oaths or where there is no such office any other person duly authorised by statute to administer oaths or to take statutory declarations in that country, such document shall be admitted in any Court in Trinidad and Tobago without proof of the seal or signature or due authorisation and such document shall be as effectual as if administered, taken or done by or before any lawful authority in Trinidad and Tobago.

(2) In any criminal proceeding any document purporting to be a certificate or report under the hand of a Government expert on any matter or thing which has been submitted to him for examination, analysis or report is admissible as evidence of the facts stated in it without proof of the signature or appointment of the Government expert, unless the Court, acting ex proprio motu or at the request of a party to the proceeding requires the expert to be called as a

witness. The Court is not bound to require the attendance of the expert as a witness if the Court is of opinion that the request for such attendance is made for the purpose of vexation, delay or defeating the ends of justice.

(2A) Where medical evidence is contained in a report signed by–

(a) a District Medical Officer, and the evidence –
(i) relates to a fatality; and
(ii) is being led in criminal proceedings or in an inquest; or

(b) a registered medical practitioner and the evidence does not relate to a fatality,

the report shall be admitted as if it were the report of a Government expert within the meaning of this section.

(3) In any inquest held by a Coroner any such certificate or report is likewise admissible as evidence of the facts stated in it unless the Coroner requires the expert to be called as a witness.

(4) In this section–

"Government expert" means the following public officers:
(a) Senior Pathologist;
(b) Pathologist;
(c) Government Chemist;
(d) Armourer;
**(e)* Forensic Document Examiner;
(f) Forensic Biologist;
(g) Scientific Examiner (Motor Vehicle);
(h) the holder of any other office or any other suitably qualified and experienced person declared by the President by Notification published in the Gazette to be an officer or person to which this section applies;

"report" includes a post mortem report.

PART IV
EVIDENCE RELATING TO BIRTHS, DEATHS AND MARRIAGES

20. (1) A certified copy of an entry in any register of births, deaths, or marriages purporting to bear the signature of the person having legal custody of such register, or of some person legally authorised to sign such copy at the time of its issue, and authenticated as provided below is, in the case of any register kept at any place in Commonwealth countries subject to all just exceptions, prima facie evidence for all purposes of the fact of the birth or death or the legal solemnisation of the marriage thereby certified.

(2) A certified copy shall bear the signature of a person describing himself as holding some office, benefice, or position entitling him to the custody of the register, or to sign such copy at the time of so certifying, and the authentication of such signature shall be under the hand and seal of a Notary Public, or under the hand of the Registrar General, or Superintendent Registrar of Births and Deaths, or Registrar of Marriages of the Commonwealth country within which such certificate purports to have been issued, or under the hand of a member of the High Court or Supreme Court of such Commonwealth country, or under the seal of a Court of civil jurisdiction in the district in which the certified copy was issued.

(3) At the preliminary examination in respect of or at any trial for any indictable offence, where it becomes necessary either for the prosecution or the defence to establish the fact of any birth, death, or marriage in any Commonwealth country, the person charged, or the wife or husband

of the person charged, may give evidence of the identity of any person with any person named in the certificate; but nothing contained in this Act shall be construed to make it compulsory on any person accused, or on his or her wife or husband, to give any such evidence if he or she is unwilling to do so.

(4) A birth, death, or marriage in the United Kingdom and the Republic of Ireland or in Trinidad and Tobago shall, saving all just exceptions, be proved in the manner provided in this section, any written law to the contrary notwithstanding.

PART V
DOCUMENTARY EVIDENCE IN CERTAIN CASES

21. In this Part–

"Government Printer" means and includes any printer purporting to be the printer authorised to print the Acts and other documents of the Government;

"document" means and includes proclamations, orders, bye-laws, rules, regulations, warrants, circulars, lists, assessment rolls, minutes, certificates, notices, requisitions, letters, decrees, and all other records and writings whatsoever of a public character pertaining to the several departments of the Government in the first column of the Second Schedule;

"bankers' books" means and includes ledgers, day books, cash books, account books, and all other books used in the ordinary business of a bank;

"legal proceeding" means any civil or criminal proceeding or enquiry in which evidence is or may be given before any Court of Justice, Judge, Magistrate or Justice, Arbitrator, Commissioner or person or persons authorised by the Supreme Court to take evidence;

"Judge" means a Judge of the Supreme Court, or of a Petty Civil

Court; "bank" and "banker" means and includes–

(a) any person or persons, partnership or company, carrying on the business of bankers in Trinidad and Tobago, or the manager;

(b) any person or persons, partnership or company, who may hereafter carry on the business of bankers in Trinidad and Tobago and who hereafter, under the authority of any Act may establish a banking association in Trinidad and Tobago, or the manager;

(c) the Post Office Savings Bank established under the Post Office Savings Bank Act. In the case of the said Savings Bank, "banker" means the Postmaster General.

22. (1) Every document issued–

(a) by the President;

(b) under the authority of the President;

(c) by or under the authority of any department of the Government or officer mentioned in the first column of the Second Schedule; or

(d) being a record in any such department of the Government,

may be received in evidence in all Courts of Justice, and in all legal proceedings whatsoever, in every case in which the original document would be admissible in evidence in all or any of the following modes:

(i) by production of a copy of the Gazette purporting to contain the document;

(ii) by production of a copy of the document purporting to be printed by the Government Printer;

(iii) by production (in the case of any document issued by the President or under the authority of the President) of a copy or extract purporting to be certified by the Minister, Secretary to the Cabinet or any Permanent Secretary; and

(iv) by production (in the case of any document issued by or under the authority of any of the departments or officer, or being a record in any such department of the Government) of a copy or extract purporting to be certified to be true by the person or persons specified in the second column of the said Second Schedule in connection with such department or officer.

Any copy or extract made in pursuance of this Part may be in print or in writing, or partly in print and partly in writing.

No proof shall be required of the handwriting or official position of any person certifying in pursuance of this Part to the truth of any copy of or extract from any document.

(2) In this section "Minister" means the Minister responsible for the subject matter in respect of which the document was issued and "Permanent Secretary" means the Permanent Secretary to the Minister.

23. No officer of any of the several public departments specified in the first column of the Second Schedule is, in any legal proceedings to which the State or he is not a party, compellable to produce any document the contents of which can be proved under this Act or to appear as a witness to prove the matters, transactions, and things recorded in it unless by order of a Judge made for special cause.

24. Any person who prints any enactment or document which falsely purports to have been printed by the Government Printer, or by the authority of the legislation or the Government of any Commonwealth territory or tenders in evidence any document which falsely purports to have been so printed knowing that the same was not so printed is liable to imprisonment for five years.

25. Section 22 shall be deemed to be in addition to and not in derogation of any powers of proving documents given by any Act or law for the time being in force in Trinidad and Tobago.

26. Subject to this Act, a copy of any entry in a banker's book shall, in all legal proceedings be received as prima facie evidence of such entry, and of the matters, transactions, and accounts therein recorded.

27. (1) A copy of an entry in a banker's book shall not be received in evidence under this Act unless it is first proved that the book was, at the time of the making of the entry, one of the ordinary books of the bank, and that the entry was made in the usual and ordinary course of business, and that the book is in the custody or control of the bank.

(2) Such proof may be given by the manager or accountant of the bank, and in the case of the Post Office Savings Bank by the Postmaster General or any person authorised by him.

(3) Such proof may be given orally, or by affidavit sworn, or statutory declaration made, before any Commissioner or person authorised to take affidavits or statutory declarations.

28. A copy of an entry in a banker's book shall not be received in evidence under this Act unless it be further proved that the copy has been examined with the original entry and is correct; such proof shall be given by some person who has examined the copy with the original entry, and may be given either orally, or by an affidavit sworn, or statutory declaration made, before any Commissioner or person authorised to take affidavits or statutory declarations.

Annex 3B

29. The manager or accountant of a bank, and in the case of the Post Office Savings Bank the Postmaster General and any person employed in connection with the Post Office Savings Bank, are not, in any legal proceeding to which the bank is not a party, compellable to produce any banker's book, the contents of which can be proved under this Act or to appear as a witness to prove the matters, transactions, and accounts recorded in it, unless by order of a Judge made for special cause.

30. On the application of any party to a legal proceeding, a Court or Judge may order that the party be at liberty to inspect and take copies of any entries in a banker's book for any of the purposes of the proceedings. An order under this section may be made either with or without summoning the bank or any other party, and shall be served on the bank three clear days, exclusive of Sundays and public holidays, before it is to be obeyed, unless the Court or Judge otherwise directs.

31. (1) There shall be paid to and taken by the officers of the departments in the Second Schedule mentioned, except the Registrar General's department, the following fees, that is to say:

For every copy of any document, for every 90

Words... ... ...

For a certificate of correctness of such copy ...

All fees under this Act shall be paid to the Comptroller of Accounts.

(2) There shall be paid to the Commissioner of Police for information relating to a road traffic accident a fee of fifty dollars.

(3) The fees specified in the Third Schedule shall be paid by private clients in respect of services provided by the Trinidad and Tobago Forensic Science Centre.

(4) The Minister may by Order amend the Third Schedule.

32. (1) In any proceeding, whether civil or criminal, an instrument as to the validity of which attestation is requisite may, instead of being proved by an attesting witness be proved in the manner in which it might be proved if no attesting witness were alive.

(2) In this section "proceedings" includes an arbitration or reference whether under any written law or not.

(3) Nothing in this section shall apply to the proof of Wills or other testamentary documents.

33. In any proceedings, whether civil or criminal, there shall, in the case of documents proved, or purporting, to be not less than twenty years old be made any presumption which immediately before 1st September 1938 would have been made in the case of a document of like character proved, or purporting, to be not less than thirty years old.

34. Nothing in section 32 or 33 shall prejudice the admissibility of any evidence which would, apart from the provisions of those sections, be admissible.

Annex 3B

PART VI
EVIDENCE IN CIVIL PROCEEDINGS

35.(1) In this Part–

"civil proceedings" includes, in addition to civil proceedings in any of the ordinary Courts of Law–

(a) civil proceedings before any other tribunal, being proceedings in relation to which the strict rules of evidence apply; and

(b) an arbitration or reference, whether under a written law or not, but does not include civil proceedings in relation to which the strict rules of evidence do not apply;

"computer" has the meaning assigned by section 40;

"Court" does not include a Court-martial, and, in relation to an arbitration or reference, means the arbitrator or umpire and, in relation to proceedings before a tribunal (not being one of the ordinary Courts of law), means the tribunal;

"document" includes, in addition to a document in writing–

(a) any map, plan, graph or drawing;

(b) any photograph;

(c) any disc, tape, sound track or other device in which sounds or other data, not being visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as mentioned above) of being reproduced therefrom;

"film" includes a microfilm;
"legal proceedings" includes an arbitration or reference, whether under a written law or not; "statement" includes any representation of fact, whether made in words or otherwise.

(2) In this Part any reference to a copy of a document includes–

(a) in the case of a document falling within paragraph (c) but not (d) of the definition of "document" in subsection (1), a transcript of the sounds or other data embodied therein;

(b) in the case of a document falling within paragraph (d) but not (c) of that definition, a reproduction or still reproduction of the image or images embodied therein, whether enlarged or not;

(c) in the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and

(d) in the case of a document not falling within the said paragraph (d) of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not,

and any reference to a copy of the material part of a document shall be construed accordingly.

(3) For the purposes of the application of this Part in relation to any such civil proceedings as are mentioned in subsection (1), any Rules of Court made for the purposes of this Act under sections 77 and 78 of the Supreme Court of Judicature Act, shall (except in so far as their operation is excluded by agreement) apply, subject to such modifications as may be appropriate, in like manner as they apply in relation to civil proceedings in the High Court of Justice.

(4) If any question arises as to what are, for the purposes of any such civil proceedings as are mentioned in subsection (1), the appropriate modifications of any such rule of Court as is mentioned in subsection (3), that question shall, in default of agreement, be determined by the tribunal or the arbitrator or umpire, as the case may be.

(5) Any reference in this Part to any other written law includes a reference thereto as applied, by or under any other written law.

(6) Nothing in this Part prejudices the operation of any written law which provides (in whatever words) that any answer or evidence given by a person in specified circumstances is not admissible in evidence against him or some other person in any proceedings or class of proceedings (however described).

(7) In subsection (6) the reference to giving evidence is a reference to giving evidence in any manner, whether by furnishing information, making discovery, producing documents or otherwise.

(8) Nothing in this Part prejudices–

(a) any power of a Court, in any legal proceeding, to exclude evidence (whether by preventing questions from being put or otherwise) at its discretion; or

(b) the operation of any agreement (whenever made) between the parties to any legal proceedings as to the evidence which is to be admissible (whether generally or for any particular purpose) in those proceedings.

(9) Where, by reason of any defect of speech or hearing from which he is suffering, a person called as a witness in any legal proceeding gives his evidence in writing or by signs, that evidence is to be treated for the purposes of this Part as being given orally.

36. (1) In any civil proceedings a statement other than one made by a person while giving oral evidence in those proceedings is admissible as evidence of any fact stated therein to the extent that it is so admissible by virtue of any provision of this Part or by virtue of any other statutory provision or by agreement of the parties, but not otherwise.

(2) In this section "statutory provision" means any provision contained in, or in an instrument made under, this or any other Act including any Act passed after the commencement of the Evidence (Amendment) Act 1973 (that is, 15th November 1973).

37.(1) In any civil proceedings a statement made, whether orally or in a document or otherwise, by any person, whether called as a witness in those proceedings or not, shall, subject to this section and to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

(2) Where in any civil proceedings a party desiring to give a statement in evidence by virtue of this section has called or intends to call as a witness in the proceedings the person by whom the statement was made, the statement–

(a) shall not be given in evidence by virtue of this section on behalf of that party without the leave of the Court; and

(b) without prejudice to paragraph (a), shall not be given in evidence by virtue of this section on behalf of that party before the conclusion of the examination-in-chief of the person by whom it was made, except–

(i) where before that person is called the Court allows evidence of the making of the statement to be given on behalf of that party by some other person; or

(ii) in so far as the Court allows the person by whom the statement was made to narrate it in the course of his examination-in-chief on the ground that to prevent him from doing so would adversely affect the intelligibility of his evidence.

(3) Where in any civil proceedings a statement which was made otherwise than in a document is admissible by virtue of this section, no evidence other than direct oral evidence by the person who made the statement or any person who heard or otherwise perceived it being made shall be admissible for the purpose of proving it, but so however, that if the statement in question was made by a person while giving oral evidence in some other legal proceedings (whether civil or criminal), it may be proved in any manner authorised by the Court.

Annex 3B

38. (1) Where in any civil proceedings –

(a) a previous inconsistent or contradictory statement made by a person called as a witness in those proceedings is proved by virtue of section 5, 6 or 7;

(b) a previous statement made by a person called as aforesaid is proved for the purpose of rebutting a suggestion that his evidence has been fabricated,

that statement shall by virtue of this subsection be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

(2) Nothing in this Part shall affect any of the rules of law relating to the circumstances in which, where a person called as a witness in any civil proceedings is cross-examined on a document used by him to refresh his memory, that document may be made evidence in those proceedings; and where a document or any part of a document is received in evidence in any such proceedings by virtue of any such rule of law, any statement made in that document or part by the person using the document to refresh his memory shall by virtue of this subsection be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

39. (1) Without prejudice to section 40, in any civil proceedings a statement contained in a document shall, subject to this section and to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if the document is, or forms part of, a record compiled by a person acting under a duty from information which was supplied by a person (whether acting under a duty or not) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with in that information and which, if not supplied by that person to the compiler of the record, directly, was supplied by him to the compiler, of the record indirectly through one or more intermediaries, each acting under a duty.

(2) Where in any civil proceedings a party desiring to give a statement in evidence by virtue of this section has called or intends to call as a witness in the proceedings the person who originally supplied the information from which the record containing the statement was compiled, the statement–

(a) shall not be given in evidence by virtue of this section on behalf of that party without the leave of the Court; and

(b) without prejudice to paragraph (a), shall not, without the leave of the Court, be given in evidence by virtue of this section on behalf of that party before the conclusion of the examination-in-chief of the person who originally supplied the said information.

(3) Any reference in this section to a person acting under a duty includes a reference to a person acting in the course of any trade, business, profession or other occupation in which he is engaged or employed or for the purposes of any paid or unpaid office held by him.

40. (1) In any civil proceedings a statement contained in a document produced by a computer shall, subject to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown that the conditions mentioned in subsection (2) are satisfied in relation to the statement and computer in question.

(2) The said conditions are–

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;

Annex 3B

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

(3) Where over a period the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2)(a) was regularly performed by computers, whether–

(a) by a combination of computers operating over that period;

(b) by different computers operating in succession over that period;

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this Part as constituting a single computer; and references in this Part to a computer shall be construed accordingly.

(4) In any civil proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say–

(a) identifying the document containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate,

and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this Part–

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) where, in the course of activities carried on by any individual or body, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

(6) Subject to subsection (3) in this Part "computer" means any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process.

41. (1) Without prejudice to the generality of section 22, where in any civil proceedings a statement contained in a document is proposed to be given in evidence by virtue of section 37, 39 or 40 it may, subject to any Rules of Court, be proved by the production of that document or (whether or not that document is still in existence) by the production of a copy of that document, or of the material part thereof, authenticated in such manner as the Court may approve.

(2) For the purpose of deciding whether or not a statement is admissible in evidence by virtue of section 37, 39 or 40 the Court may draw any reasonable inference from the circumstances in which the statement was made or otherwise came into being or from any other circumstances, including, in the case of a statement contained in a document the form and contents of that document.

(3) In estimating the weight, if any, to be attached to a statement admissible in evidence by virtue of section 37, 38, 39 or 40 regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular–

(a) in the case of a statement falling within section 37(1) or 38(1) or (2), to the question whether or not the statement was made contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not the maker of the statement had any incentive to conceal or misrepresent the facts;

(b) in the case of a statement falling within section 39(1), to the question whether or not the person who originally supplied the information from which the record containing the statement was compiled did so contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not that person, or any person concerned with compiling or keeping the record containing the statement, had any incentive to conceal or misrepresent the facts; and

(c) in the case of a statement falling within section 40(1) to the question whether or not the information which the information contained in the statement reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied thereto, contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.

(4) For the purpose of any written law or rule of law or practice requiring evidence to be corroborated or regulating the manner in which uncorroborated evidence is to be treated–

(a) a statement which is admissible in evidence by virtue of section 37 or 38 shall not be capable of corroborating evidence given by the maker of the statement; and

(b) a statement which is admissible in evidence by virtue of section 8 shall not be capable of corroborating evidence given by the person who originally supplied the information from which the record containing the statement was compiled.

(5) Any person who, in a certificate tendered in evidence in civil proceedings by virtue of section 40(4), wilfully makes a statement material in those proceedings which he knows to be false or does not believe to be true is liable on conviction on indictment to a fine and to imprisonment for two years.

42. (1) Subject to Rules of Court, where in any civil proceedings a statement made by a person who is not called as a witness in those proceedings is given in evidence by virtue of section 37 –

(a) any evidence which, if that person had been so called, would be admissible for the purpose of destroying or supporting his credibility as a witness shall be admissible for that purpose in those proceedings; and

(b) evidence tending to prove that, whether before or after he made that statement, that person made (whether orally or in a document or otherwise) another statement inconsistent therewith shall be admissible for the purpose of showing that that person has contradicted himself.

(2) Nothing in subsection (1) shall enable evidence to be given of any matter of which, if the person in question had been called as a witness and had denied that matter in cross-examination, evidence could not have been adduced by the cross-examining party.

(3) Subsection (1) shall apply in relation to a statement given in evidence by virtue of section 39 as it applies in relation to a statement given in evidence by virtue of section 37, except that references to the person who made the statement and to his making the statement shall be construed, respectively, as references to the person who originally supplied the information from which the record containing the statement was compiled and to his supplying that information.

(4) Section 38(1) shall apply to any statement proved by virtue of subsection (l)(b) as it applies to a previous inconsistent or contradictory statement made by a person called as a witness which is proved as mentioned in paragraph (a) of the said section 38(1).

43. (1) Provision shall be made by Rules of Court as to the procedure which, subject to any exceptions provided for in the Rules, must be followed and the other conditions which, subject as aforesaid, must be fulfilled before a statement can be given in evidence in civil proceedings by virtue of section 37, 39 or 40.

(2) Rules of Court made in pursuance of subsection (1) shall in particular, subject to such exceptions (if any) as may be provided for in the Rules–

(a) require a party to any civil proceedings who desires to give in evidence any such statement as is mentioned in that subsection to give to every other party to the proceedings such notice of his desire to do so and such particulars of or relating to the statement as may be specified in the Rules, including particulars of such one or more of the persons connected with the making or recording of the statement or, in the case of a statement falling within section 37(1), such one or more of the persons concerned as mentioned in section 41(3)(c) as the Rules may in any case require; and

(b) enable any party who receives such notice as aforesaid by counter-notice to require any person of whom particulars were given with the notice to be called as a witness in the proceedings; unless that person is dead, or beyond the seas, or unfit by reason of his bodily or mental condition to attend as a witness, or cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which has elapsed since he was connected or concerned as aforesaid and to all the circumstances) to have any recollection of matters relevant to the accuracy or otherwise of the statement.

(3) Rules of Court made in pursuance of subsection (1)–

(a) may confer on the Court in any civil proceedings a discretion to allow a statement falling within section 37(1), 39(1) or 40(1) to be given in evidence notwithstanding that any requirement of the rules affecting the admissibility of that statement has not been complied with; except in pursuance of paragraph (b), Rules of Court may not confer on the Court a discretion to exclude such a statement where the requirements of the rules affecting its admissibility have been complied with;

(b) may confer on the Court power, where a party to any civil proceedings has given notice that he desires to give in evidence –

(i) a statement falling within section 37(1) that was made by a person, whether orally or in a document, in the course of giving evidence in some other legal proceedings (whether civil or criminal); or

(ii) a statement falling within section 39(1) that is contained in a record of any direct oral evidence given in some other legal proceedings (whether civil or criminal), to give directions on the application of any party to the proceedings as to whether, and if so on what conditions, the party desiring to give the statement in evidence will be permitted to do so (where applicable) as to the manner in which that statement and any other evidence given in those other proceedings is to be proved; and

(c) may make different provision for different circumstances, and in particular may make different provisions with respect to statements falling within sections 37(1), 39(1) and 40(1), respectively,

and any discretion conferred on the Court by Rules of Court made in accordance with this section may be either a general discretion or a discretion exercisable only in such circumstances as may be specified in the Rules.

(4) Rules of Court may make provision for preventing a party to any civil proceedings (subject to any exceptions provided for in the Rules) from adducing in relation to a person who is not called as a witness in those proceedings any evidence that could otherwise be adduced by him by virtue of section 42, unless that party has in pursuance of the Rules given in respect of that person such a counter-notice as is mentioned in subsection (2)*(b)*.

(5) In deciding for the purposes of any Rules of Court made in pursuance of this section whether or not a person is fit to attend as a witness, a Court may act on a certificate purporting to be a certificate of a registered medical practitioner.

(6) Nothing in the foregoing provisions of this section shall prejudice the generality of section 76 of the Supreme Court of Judicature Act, or any other written law conferring power to make Rules of Court; and nothing in any enactment restricting the matters with respect to which Rules of Court may be made shall prejudice the making of Rules of Court with respect to any matter mentioned in the foregoing provisions of this section or the operation of any Rules of Court made with respect to any such matter.

44. (1) In any civil proceedings a statement which, if this Part had not been passed, would by virtue of any rule of law mentioned in subsection (2) have been admissible as evidence of any fact stated therein shall be admissible as evidence of that fact by virtue of this subsection.

(2) The rules of law referred to in subsection (1) are the following, that is to say any rule of law:

(a) whereby in any civil proceedings an admission adverse to a party to the proceedings, whether made by that party or by another person, may be given in evidence against that party for the purpose of proving any fact stated in the admission;

(b) whereby in any civil proceedings published works dealing with matters of a public nature (for example, histories, scientific works, dictionaries and maps) are admissible as evidence of facts of a public nature stated therein;

(c) whereby in any civil proceedings public documents (for example, public registers, and returns made under public authority with respect to matters of public interest) are admissible as evidence of facts stated therein; or

(d) whereby in any civil proceedings records (for example, the records of certain Courts, treaties, State grants, pardons and commissions) are admissible as evidence of facts stated therein.

In this subsection “admission” includes any representation of fact, whether made in words or otherwise.

(3) In any civil proceedings a statement which tends to establish reputation or family tradition with respect to any matter and which, if this Part had not been passed, would have been admissible in evidence by virtue of any rule of law mentioned in subsection (4)–

(a) shall be admissible in evidence by virtue of this paragraph in so far as it is not capable of being rendered admissible under section 37 or 39; and

(b) if given in evidence under this Act (whether by virtue of paragraph (a) or otherwise) shall by virtue of this paragraph be admissible as evidence of the matter reputed or handed down,

and, without prejudice to paragraph (b), reputation shall for the purposes of this Act be treated as a fact and not as a statement or multiplicity of statements dealing with the matter reputed.

(4) The rules of law referred to in subsection (3) are the following, that is to say any rule of law:

(a) whereby in any civil proceedings evidence of a person's reputation is admissible for the purpose of establishing his good or bad character;

(b) whereby in any civil proceedings involving a question of pedigree or in which the existence of a marriage is in issue, evidence of reputation or family tradition is admissible for the purpose of proving or disproving pedigree or the existence of the marriage, as the case may be; or

(c) whereby in any civil proceedings evidence of reputation or family tradition is admissible for the purpose of proving or disproving the existence of any public or general right or of identifying any person or thing.

(5) It is hereby declared that in so far as any statement is admissible in any civil proceedings by virtue of subsection (1) or (3)(a), it may be given in evidence of those proceedings notwithstanding anything in sections 37 to 42 or in any Rules of Court made in pursuance of section 43.

(6) The words in which any rules of law mentioned in subsection (2) or (4) is there described are intended only to identify the rule in question and shall not be construed as altering that rule in any way.

45. (1) In any civil proceedings–

(a) the fact that a person has been found guilty of, or to have committed, adultery in any matrimonial proceedings; and

(b) the fact that a person has been adjudged to be the father of a child in affiliation proceedings before any Court in Trinidad and Tobago,

shall [subject to subsection (3)] be admissible in evidence for the purpose of proving, where to do so is relevant to any issue in those civil proceedings, that he committed the adultery to which the finding relates, or, as the case may be, is (or was) the father of that child, whether or not he offered any defence to the allegation of adultery or paternity and whether or not he is a party to the civil proceedings; but no finding or adjudication other than a subsisting one shall be admissible in evidence by virtue of this section.

(2) In any civil proceedings in which by virtue of this section a person is proved to have been found guilty of, or to have committed, adultery as mentioned in subsection (l)(a) or to have been adjudged to be the father of a child as mentioned in subsection (l)(b)–

(a) he shall be taken to have committed the adultery to which the finding relates or, as the case may be, to be (or have been) the father of that child, unless the contrary is proved; and

(b) without prejudice to the reception of any other admissible evidence for the purpose of identifying the facts on which the finding or adjudication was based, the contents of any document which was before the Court or which contains any pronouncement of the Court, in the matrimonial or affiliation proceedings in question shall be admissible in evidence for that purpose.

(3) Nothing in this section shall prejudice the operation of any enactment whereby a finding of fact in any matrimonial or affiliation proceedings is for the purposes of any other proceedings made conclusive evidence of any fact.

46. (1) The following rules of law are hereby abrogated except in relation to criminal proceedings, that is to say:

(a) the rule whereby, in any legal proceedings, a person cannot be compelled to answer any question or produce any document or thing if to do so would tend to expose him to a forfeiture; and

(b) the rule whereby, in any legal proceedings, a person other than a party to the proceedings cannot be compelled to produce any Deed or other document relating to his title to any land.

(2) The rule of law whereby, in any civil proceedings, a party to the proceedings cannot be compelled to produce any document relating solely to his own case and in no way tending to impeach that case or support the case of any opposing party is hereby abrogated.

47. This Act binds the State.

Annex 3C:

LMM(02)12
COMMONWEALTH DRAFT MODEL LAW ON ELECTRONIC EVIDENCE

1. Law Ministers and Attorney-Generals of Small Commonwealth Jurisdictions, at their 2000 meeting, recognized that common law rules of evidence were not adequate to deal with technological advances and needed to be modernised. They welcomed the convening of an Expert Group to develop model legislation on electronic evidence to address the needs of small Commonwealth jurisdictions.

2. The Expert Group examined the admissibility of electronic evidence and the question whether the rules that apply to other forms of documentary evidence can be applied in a like manner to electronic documents. Computer records are sophisticated systems that may be more prone or vulnerable to alteration and degradation than are records on paper. Therefore it was thought that the admissibility rule should take account of this risk. The Group noted that most jurisdictions seeking to impose a minimum level of reliability for admissibility of documents do so by focusing not on the document itself but rather on the method (system) by which the document was produced. This is because it is very difficult to show anything about the electronic document per se. By showing the reliability of the system one can lay the basis for admissibility of the document which is the product of that system. The Group agreed that system reliability is the most sensible measurement.

3. The model law contains provisions on general admissibility, the scope of the model law, authentication, application of best evidence rule, presumption of integrity, standards, proof by affidavit, cross examination, agreement on admissibility of electronic records, and admissibility of electronic signature.

4 On the basis of these deliberations, the Commonwealth Secretariat decided that because of the complexity of the issues, a separate model law on electronic evidence should be drawn up in order to ensure admissibility of such evidence. The model law draws on the Singapore Evidence Act Section 35 (1), the Canada Uniform Electronic Evidence Act and UNCITRAL Model Law on E-Commerce. Member countries wishing to make use of the model E-Evidence Law may choose to do so as–

- a separate piece of legislation; or
- part of a law on electronic transactions; or
- as amendments to existing laws on evidence; or
- as an addition to the proposals contained in paper LMM(02)4 which deals with modernisation of evidence laws but concentrates primarily on criminal law matters and business records in their more traditional sense.

5. The model provisions on electronic evidence are annexed to this paper.

ACTION BY LAW MINISTERS

2

6. Law Ministers may wish to endorse the annexed Electronic Evidence Model Law and commend it to member countries for adoption (or adaptation to national circumstances) as a Commonwealth model of good practice.

Annex 3C

Commonwealth Secretariat
Marlborough House
London SW1Y 5HX September 2002

ANNEX

ELECTRONIC EVIDENCE MODEL LAW

AN ACT to make provision for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings.

BE IT ENACTED by the Parliament *[name of legislature]* of …… *[name of country]* as follows: Short Title 1. This Act may be cited as the Electronic Evidence Act, 2002

Interpretation 2. In this Act,

"data" means representations, in any form, of information or concepts;

"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records.

"legal proceeding" means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

General Admissibility

3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

4. (1) This Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence.

Scope of Act (2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

Authentication 5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

4

Application of Best Evidence Rule

6. (1) In any legal proceeding, subject to subsection (b), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.

Annex 3C

Presumption of Integrity

7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) Where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record.

(b) Where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) Where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards 8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Proof by Affidavit

9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross Examination

10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in subsection 7(c).

5

Agreement on Admissibility of Electronic Records

11. (1) Unless otherwise provided in any other statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a solicitor.

Admissibility of Electronic Signature

12. (1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

Annex 3D:

SAINT VINCENT AND THE GRENADINES
ELECTRONIC TRANSACTIONS ACT, 2007

ARRANGEMENT OF SECTIONS

Annex 3D

Annex 3D

SAINT VINCENT AND THE GRENADINES

BILL FOR

_____

ACT NO. OF 2007

I ASSENT

Governor-General

AN ACT to provide for the facilitation and regulation of electronic communications and transactions, to prevent abuse of information systems and to provide for matters BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the House of Assembly of Saint Vincent and the Grenadines and by the authority of the same, as follows:

PART I
PRELIMINARY

1. This Act may be cited as the Electronic Transactions Act, 2007 and shall come into operation on a day appointed by the Governor-General by Proclamation in the Gazette.

2. In this Act:

"addressee" means a person who is intended by the originator to receive data message but does not include a person acting as intermediary in respect of the

"advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Accreditation Authority as provided for in section 29;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services have been accredited by the Accreditation Authority under section 29 or recognised under section 32;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or

"consumer" means any natural person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"critical information system" means a collection of critical information in electronic form from where it may be accessed, reproduced or extracted;

"critical information systems administrator" means the person responsible for the management and control of a critical information system;

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the

(a) that the data can be accessed only by relevant persons;
(b) the authenticity of the data;
(c) the integrity of the data;
(d) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides or who proposes to provide cryptograph services or products in the State;

"cryptography service" means any service which is provided to a sender or recipient of a data message or to anyone storing a data message, and is designed to facilitate the use of cryptographic techniques for the purpose of

(a) that the data or data message can be accessed or can be put into an intelligible form only by certain persons;

(b) that the authenticity or integrity of the data or data message is capable of

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained;

"cyber inspector" means a person appointed under Part V;

"data" means electronic representations of information in any form;

"data message" means data generated, received or stored by electronic means and

(a) a voice, where the voice is used in an automated transaction;

(b) a stored record;

"electronic" means created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or by any other means that has capabilities for creation, recording, transmission or storage similar to those

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the internet and wireless application protocol communications;

"public authority" includes–

(a) Parliament, or any committee of Parliament;

(b) the Cabinet as constituted under the Constitution;

(c) a Ministry or a department or division of a Ministry;

(d) a local authority;

(e) a public statutory corporation or body;

(f) a body corporate or an incorporated body established for a public purpose, which is owned or controlled by the State;

(g) an embassy, consulate or mission of the State or any office of the State situated outside of Saint Vincent and the Grenadines whose functions include the provision of diplomatic or consular services for or on behalf of Saint Vincent and the Grenadines;

(h) any other body designated by the Minister by Regulation made under this Act, to be a public authority for the purposes of this Act;

"Minister" means the Minister responsible for telecommunications;

"Ministry" means the Ministry responsible for telecommunications;

"rule of law" means the common law, an Act of Parliament or legislation made under an Act of Parliament;

"signature creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic

"State" means Saint Vincent and the Grenadines;

"website" or "web portal" means any computer on the internet containing a home

3. This Act shall bind the Crown.

PART II
LEGAL REQUIREMENTS FOR ELECTRONIC TRANSACTIONS

4. (1) Information shall not be denied legal effect, validity or enforcement solely on the ground that it is in electronic form.

(2) In sections 5, 6, 7, 8 and 22:

(a) where a rule of law require information to be in writing, given, signed, original or retained, the requirement is met if the section is complied with;

(b) where a rule of law provides consequences where the information is not in writing, given, signed, original or retained, the consequences are avoided if the section is complied with; and

(c) where a rule of law provides consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.

5. (1) A rule of law that requires information to be in writing or to be given in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.

(2) In subsection (1), giving information includes, but is not limited to, the

(a) making an application;

(b) making, filing or lodging a claim;

(c) giving, sending or serving a notification;

(d) filing or lodging a return;

(f) making a declaration;

(g) filing, lodging or issuing a certificate;

(h) making, varying or cancelling an election; (i) filing or lodging an objection;

(j) giving a statement of reasons.

(3) Information in electronic form is not given unless the information is capable of being retained by the person to whom it is given.

6. (1) A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in

(a) organized in the same or substantially the same way as the prescribed non-

(b) accessible to the other person so as to be usable for subsequent reference;

(c) capable of being retained by the other person.

7. A rule of law that requires a person to produce, examine or keep an original document is satisfied if the person produces, examines or retains the document in

(a) having regard to all the relevant circumstances, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the

(b) in a case where an original document is to be given to the person in electronic form is accessible so as to be usable for subsequent reference and capable of being retained by the person.

8. A rule of law that requires a person to keep information that is in writing or that is in electronic form, is satisfied by keeping the information in electronic form, if:

(a) having regard to all the relevant circumstances when the electronic form of the document was generated, the method of generating the electronic form of the document provided a

reliable means of assuring the maintenance of the integrity of the information contained in the document;

(b) when the electronic form of the document was generated, the information contained in the electronic form of the document is accessible so as to be usable for subsequent reference to any person entitled to have access to the information or to require its production.

9. For the purposes of sections 7 and 8 the soundness of the information has remained complete and unaltered, apart from:

(a) the addition of any endorsement; or

(b) any immaterial change;

which arises in the normal course of communications, storage or display.

10.(1) If a public authority has power to create, collect, receive, store, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the (2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

(3) For the purposes of subsection (2) a reference to writing or signature does not in itself constitute an express prohibition of the use of electronic means.

(4) Where a public authority consents to receive any information in electronic

(a) the manner, and format in which the information shall be communicated to

(b) the type or method of electronic signature required, if any;

(c) control processes and procedures to ensure integrity, security and confidentiality of the information;

(d) any other attributes for the information that are currently specified for corresponding information on paper.

(5) The requirements of subsections (1) and (3) and section 6 also apply to information described in subsection (4) of this section.

(6) A public authority may make or receive payment in electronic form by any manner specified by the authority and approved by the Minister of Finance.

11.(1) Where a rule of law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, the requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a rule of law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, the requirement is met if the person provides a print-out certified to be a true reproduction of the document or

(3) Where a rule of law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, the requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

12. (1) A requirement in a rule of law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a rule of law, whether used as a noun or verb, including the terms, “document”, “record”, “file”, “submit”, “lodge”, “deliver”, “issue”, “publish”, “write in”, “print” or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless

(3) Where a seal is required by a rule of law to be affixed to a document and the law does not prescribe the method or form by which the document may be sealed by electronic means, the requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is

(4) Where a rule of law requires or permits a person to send a document by registered or certified post, the requirement is met if an electronic copy of the document or information is sent to, is registered by and sent by the Saint Vincent and the Grenadines Postal Corporation to the electronic address.

13. This Act does not apply to:

(a) the creation or transfer of interests in real property;

(b) negotiable instruments;

(c) Documents title;

(d) wills and trusts created by wills;

(e) any class of documents, transactions or rules of law excluded by Regulation under this Act.

14. (1) Nothing in this Act limits the operation of any other rule of law that expressly authorizes, prohibits or regulates the use of information in electronic form including a method of electronic or advanced electronic signature.

(2) Nothing in this Act limits the operation of any other rule of law requiring information to be posted or displayed in a specific manner or requiring information to be transmitted by a specified method.

(3) A reference to writing or signature does not itself constitute a prohibition for the purpose of subsection (1) or a legal requirement for the purpose of subsection (2).

15. (1) Nothing in this Act requires a person to use, provide or accept information in electronic form without consent, but a person's consent to do so may be inferred from the

(2) Notwithstanding subsection (1), the consent of a public authority to accept information in electronic form may not be inferred from its conduct but must be expressed by communication accessible to the public or to those most likely to communicate with it for particular purposes.

(3) Nothing in this Act authorises a public authority to require any person to use, provide or accept information in electronic form without consent.

16. (1) Unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed:

(a) by means of information in electronic form; or

(b) by an act that is intended to result in electronic communication, such as touching or clicking an appropriate icon or other place on a computer screen, or by speaking.

(2) A contract is not invalid or unenforceable by reason only of being in

17. A contract may be formed by interaction of computer programmes or other electronic means used to initiate an act or to respond to electronic information, in whole or in part, without review by an individual at the time of the response or act.

18. (1) An electronic transaction between an individual and another person's automated source of information has no legal effect if:

(a) the individual makes a material error in electronic information or an electronic document used in the transaction;

(b) the automated source of information does not give the individual an opportunity to prevent or correct the error;

(c) on becoming aware of the error, the individual promptly notifies the other

(d) in a case where consideration is received as a result of the error, the individual, returns or destroys the consideration in accordance with the other person's instructions, deals with the consideration in a reasonable manner, and does not benefit materially by receiving the consideration.

(2) This section does not limit any other rule of law relating to mistake.

19. Betwen the originator and the addressee of a communication in electronic form, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form.

20.(1) An electronic communication is sent when it enters an information system outside the sender's control or, if the sender and the addressee use the same information system, when it becomes capable of being retrieved and processed by the addressee.

(2) An electronic communication is presumed to be received by the addressee:

(a) if the addressee has designated or uses an information system for the purposes of receiving communications of the type sent, when it enters that information system and becomes capable of being retrieved and processed by the addressee; or

(b) if the addressee has not designated or does not use an information system for the purpose of receiving communications of the type sent, or if the addressee has designated or used such a system but the communication has been sent to another system, when the addressee becomes aware of the communication in the addressee's information system and it becomes capable of being retrieved and processed by the addressee.

(3) Subsections (1) and (2) apply unless the parties agree otherwise.

(4) An electronic communication is deemed to be sent from the sender's place of business and received at the addressee's place of business.

(5) If the sender or addressee has more than one place of business, the place of business for the purpose of subsection (4) is the one with the closest relationship to the underlying transaction to which the electronic communication relates or, if there is no underlying transaction, the person's principal place of business.

(6) If the sender or addressee does not have a place of business, the person's place of habitual residence is deemed to be the place of business for the purposes of subsection (4)

21. An electronic communication is that of the person who sends it, if it is sent directly by the person or by an information system programmed by on behalf of the

PART III ELECTRONIC SIGNATURES

22. (1) If a rule of law requires the signature of a person, the requirement is met by an electronic signature if the electronic signature that is used is as reliable and as appropriate for the purpose for which it was generated or communicated, in all the circumstances, including any relevant agreements.

(2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the rule of law provides consequences for the absence of a signature.

(3) An electronic signature is not without legal force and effect merely on the

(4) Parties may agree to use a particular method of electronic signature, unless

(5) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, the requirement is met in relation to the data message if:

(a) the signature creation data is linked to the signatory and no other person;

(b) the signature creation data at the time of signing is under the control of the signatory and no other person;

(c) any alteration to the electronic signature, made after the time of signing is

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the soundness of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(6) Subsection (5) does not limit the ability of a person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

23. The Minister may make Regulations prescribing methods which satisfy the

24. A person relying on an electronic signature shall bear the legal consequences of his failure to take reasonable steps to verify the reliability of an electronic signature.

25. In determining whether or to what extent information in electronic form is legally effective, no regard shall be had to the location where the information was created or used, or to the place of business of its creation.

PART IV
ACCREDITATION

26. In this Part, unless the context indicates otherwise:

"accreditation" means recognition of an authentication product or service by the Accreditation Authority.

27.(1) For the purposes of this Part the Minister shall be the Accreditation Authority.

(2) Public officers may be appointed or designated as Deputy Accreditation Authorities and officers of the Accreditation Authority.

28.(1) The Accreditation Authority may–

(a) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this Act;

(b) temporarily suspend or revoke the accreditation of an authentication product or service; and

(c) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this

(2) The Accreditation Authority shall maintain a publicly accessible database in

(a) authentication products or services accredited in terms of section 30;

(b) authentication products and services recognised in terms of section 32;

(c) revoked accreditations or recognitions; and

(d) any other information as may be prescribed.

29.(1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation shall–

(a) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and

(b) accompanied by a non-refundable prescribed fee.

Annex 3D

(3) A person who falsely holds out its products or services to be accredited by the Accreditation Authority commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars.

30.(1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate:

(a) is uniquely linked to the user;

(b) is capable of identifying the user;

(c) is created using means that can be maintained under the sole control of the

(d) will be linked to the information to which it relates in such a manner that any subsequent change of the information is detectable; and

(e) is based on the face-to face identification of the user.

(2) For the purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:

(a) its financial and human resources including its assets;

(b) the quality of its hardware and software systems;

(c) its procedures for processing of products and services;

(d) the availability of information to third parties relying on the authentication

(e) the regularity and extent of audits by an independent body;

(f) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and

(g) any other relevant factor that may be prescribed.

(3) For the purposes of subsection (2) (b) and (c), the hardware and software systems and procedures must at least:

(a) be reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation;

(c) be reasonably suited to performing their intended functions; and

(d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services:

(a) the technical and other requirements which certificates must meet;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities of the certification service provider;

(e) the liability of the certification service provider;

(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements as to adequate certificate suspension and revocation

(h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

Annex 3D

31.(1) The Accreditation Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 30 or recognition was given in terms of section 32.

(2) Subject to the provisions of subsection (3), the Accreditation Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1)

(a) notified the authentication service provider in writing of the intention to

(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 30 or recognition was given in terms of section 32; and

(c) afforded the authentication service provider the opportunity to–

(i) respond to the allegations in writing,

(ii) remedy the alleged breach within a reasonable time.

(3) The Accreditation Authority may suspend accreditation granted under section 30 or recognition given in terms of section 32 with immediate effect for a period not exceeding 90 days, pending implementation of procedures required by subsection (2) of this section, if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in Saint Vincent and the Grenadines.

(4) An authentication service provider whose products or services have been accredited under the terms of this Act may terminate the accreditation at any time, subject to terms and conditions as may be agreed to at the time of accreditation or thereafter.

32.(1) The Minister, may, by notice in the Gazette and subject to conditions as may be determined by him, recognise the accreditation or similar recognition granted to an authentication service provider or its authentication products or services in any foreign

(2) An authentication service provider who falsely holds out its products or services to have been recognised by the Minister commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars.

33. The Minister may make Regulations in respect of:

(a) the rights and obligations of persons relating to the provision of accredited products and services;

(b) the manner in which the Accreditation Authority must administer and supervise compliance with the obligations in relation to paragraph (a);

(c) the procedure pertaining to the granting, suspension and revocation of

(e) information security requirements or guidelines; and

(f) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Part.

PART V CRYPTOGRAPHY PROVIDERS

34.(1) The Minister shall establish and cause to be maintained a register of

(2) The following particulars in respect of a cryptography provider shall be

(a) the name and address of the cryptography provider;

(b) a description of the type of cryptography service or product being

(c) any other particulars as may be prescribed to adequately identify and locate the cryptography provider and its products or services.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

35.(1) A person shall not provide cryptography services or products in the State until he is registered as a cryptography provider.

(2) A cryptography provider shall in the prescribed manner provide the Minister with the information required and pay the prescribed fee.

(3) For the purposes of subsection (1), a cryptography service or product is regarded as being provided in the State if it is provided:

(a) from premises in the State;

(b) to a person who is present in the State when that person makes use of the service or product;

or

(c) to a person who uses the service or product for the purposes of a business carried on in the State or from premises in the State.

36.(1) Information contained in the database in respect of section 32 shall not be disclosed to any other person other than the officers of the Accreditation Authority who are responsible for keeping the database.

(2) Subsection (1) shall not apply in respect of information which is disclosed:

(a) to a relevant authority which investigates a criminal offence or for the purposes of criminal proceedings;

(b) to government agencies responsible for safety and security in the State pursuant to an official request;

(c) to a cyber inspector;

(d) pursuant to the provisions of the Freedom of Information Act 2003; or

(e) for the purposes of any civil proceedings which relate to the provision of cryptography services or products and to which a cryptography provider is

PART VI CONSUMER PROTECTION

37.(1) This Part applies only to electronic transactions.

(2) This Part does not apply to a regulatory authority established under a rule of law if that rule of law prescribes consumer protection provisions in respect of electronic

38.(1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following information available to consumers:

(a) its full name and legal status;

(b) its physical address and telephone number; (c) its web site address and e-mail address;

(d) the physical address where the supplier will receive legal service of

(e) a sufficient description of the main characteristics of the goods or services offered by the supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

(f) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(g) the manner of payment;

(h) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;

(i) the time within which the goods will be dispatched or delivered or within which the services will be rendered;

(j) the manner and period within which consumers can access and maintain a full record of the transaction;

(k) the return, exchange and refund policy of the supplier;

(l) the security procedures and privacy policy of the supplier in respect of payment, payment information and personal information; and

(m) the rights of consumers under section 36, where applicable.

(2) The supplier shall provide a consumer with the opportunity:

(a) to review the entire electronic transaction;

(b) to correct any mistakes; and

(c) to withdraw from the transaction before finally placing any order.

(3) If the supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services

(4) If a transaction is cancelled as provided by subsection (3):

(a) the consumer shall return the goods of the supplier or, where applicable, cease using the services performed; and

(b) the supplier shall refund all payments made by the consumer including the cost of returning the goods.

(5) The supplier shall utilize a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type

(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

39.(1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply:

(a) of goods within 7 days after the date of receipt of the goods; or

(b) of services within 7 days after the date of conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund shall be made within 30 days of the date of cancellation.

(4) This section does not apply to an electronic transaction:

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

(b) by way of an auction;

(c) for the supply of food stuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of

(d) for services which began with the consumer's consent before the end of the seven day period referred to in subsection (1);

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) Where the goods:

(i) are made to the consumer's specifications,

(ii) are clearly personalised,

(iii) by reason of their nature cannot be returned, or

Annex 3D

(iv) are likely to deteriorate or expire rapidly;

(g) where audio or video recordings or computer software were unsealed by

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

(5) This section must not be construed as prejudicing the rights of a consumer

40.(1) A person who sends unsolicited commercial communications to consumers

(a) the option to cancel his subscription to the mailing list of that person; and

(b) the identifying particulars of the source from which that person obtained the consumer's personal information, on the request of the consumer.

(2) Where a consumer fails to respond to an unsolicited commercial communication, no agreement is considered to be concluded.

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars.

(4) A person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcomed, commits an offence and is liable upon summary conviction to a fine not exceeding six thousand dollars.

41. The protection provided to consumers in this Part applies irrespective of the legal system applicable to the agreement in question.

42. Any provision in an agreement which excludes any rights provided for in this Part

43. A consumer may lodge a complaint with the appropriate consumer protection body in respect of non-compliance with the provisions of this Part by a supplier.

PART VII
PROTECTION OF CRITICAL INFORMATION SYSTEMS

44. The provisions of this Part only apply to critical information systems of public

45. The Minister may by notice in the Gazette:

(a) declare certain classes of information which are of importance to the protection of the national security of Saint Vincent and the Grenadines or the economic and social well-being of its citizens to be critical information for the purposes of this Part;

(b) establish procedures to be followed in the identification of critical information systems for the purposes of this Part.

46.(1) The Minister may by notice in the Gazette determine:

(a) requirements for the registration of critical information systems with the Ministry or such other body as the Minister may specify;

(b) procedures to be followed for registration; and

(c) any other matter relating to registration.

(2) For the purposes of this Part, registration of critical information systems means recording the following information in a register maintained by the Ministry or by such other body as the Minister may specify:

(a) the full name, address and contact details of the critical information system administrator;

(b) the location of the critical information system including the location of component parts thereof where a critical information system is not stored at a single location; and

(c) a general description of the categories or types of information stored in the system excluding the contents of such system.

47.(1) The Minister may prescribe minimum standards or prohibitions in respect of:

(a) the general management of critical information systems;

(b) access to, transfer and control of critical information systems;

(c) infrastructural or procedural rules and requirement for securing the integrity and authenticity of critical information;

(d) procedures and technological methods to be used in the storage or archiving of critical information systems;

(e) disaster recovery plans in the event of loss of critical information systems

(f) any other matter required for the adequate protection, management and control of critical information systems.

(2) This Part must not be construed so as to prejudice the right of a public authority to perform any function authorised in terms of any other law.

48.(1) Information contained in the register provided for in section 46 must not be disclosed to any other person than to employees of the Ministry or body who are responsible for keeping the register.

(2) Subsection (1) does not apply in respect of information which is disclosed:

(a) to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;

(b) to public authorities responsible for safety and security in Saint Vincent and the Grenadines pursuant to an official request;

(c) to an independent auditor for the purposes of section 49;

(d) pursuant to the provisions of the Freedom of Information Act, 2003;

(e) for the purposes of any civil proceedings which relate to the critical information system or parts thereof.

49.(1) The Minister may, from time to time, cause audits to be performed in relation to critical information systems to evaluate compliance with Regulations made under this

(2) The audit may be performed by an independent auditor.

50. Where the audit performed under section 49 reveals non-compliance with this Part, the Minister shall notify the critical information system administrator in writing of

(a) the finding of the audit report;

(b) the action required to remedy the non-compliance; and

(c) the period within which the remedial action must be performed.

PART VIII
LIABILITY OF SERVICE PROVIDERS

51. In this Part, “service provider” means any person providing information system

52.(1) The Minister may, on application by an industry representative body for service providers, by notice in the Gazette, recognise the body.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that:

(a) its members are subject to a code of conduct;

(b) the code of conduct requires continued adherence to adequate standards of

(c) the representative body is capable of monitoring and enforcing its code of conduct adequately.

53. The limitations on liability established by this Part apply to a service provider

(a) the service provider is a member of the representative body referred to in

(b) the service provider has adopted and implemented the official code of conduct of that representative body.

54.(1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider:

(a) does not initiate the transmission; (b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection

(d) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted inso far as this takes place:

(a) for the sole purpose of carrying out the transmission in the information

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients;

and

(c) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

55.(1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider:

(a) does not modify the data;

(c) complies with the conditions on access to the data;

(c) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by the industry;

(d) does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain information on the use of data; and

(e) removes or disables access to the data it has stored upon receiving a notification referred to in section 57.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in the terms of any other law.

56.(1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider:

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(b) is not aware of facts or circumstances from which infringing activity or the infringing nature of the data message is apparent; and

(c) upon receipt of a notification referred to in section 57, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to deal with notifications of infringement and has provided through its services, including on its websites, in locations accessible to the public, the name, address, phone number and e- mail address of the agent.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent an unlawful activity in terms of any other law.

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority of the control of the service provider.

57.(1) The Minister shall issue a notification of unlawful activity to a service provider upon receiving a complaint by a complainant.

(2) For the purposes of this Part, notification of unlawful activity shall be in writing and be addressed to the service provider or its designated agent and must include:

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be subject of

(e) the remedial action required to be taken by the service provider in respect

(f) telephonic and electronic contact details, if any, of the complainant; (g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take down notification is to his knowledge true and correct; and

(i) an undertaking given by the complainant to indemnify the service provider from any liability incurred as a result of remedial action taken by it in complying with the notification.

58. When providing the services contemplated in this Part, there is no general obligation of a service provider to:

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

59. This part does not affect:

(a) any obligation founded on an agreement;

(b) the obligation of a service provider under a licensing or other regulatory

PART IX CYBER INSPECTORS

60.(1) An officer of the Ministry or any other qualified person may be appointed as a cyber inspector to perform the functions provided for in this Part.

(2) A cyber inspector must be provided with a certificate of appointment signed by or on behalf of the Minister in which it is stated or evidenced that he is appointed as a

(3) A certificate provided for in subsection (2) may be in the form of an advanced

(4) When a cyber inspector performs any function in terms of this Act, he shall:

(a) be in possession of a certificate of appointment referred to in subsection (2) and;

(b) show that certificate to any person who–

(i) is subject to an investigation or an employee of that person, or

(ii) requests to see the certificate.

(5) A person who:

(a) hinders or obstructs a cyber inspector in the performance of his functions;

(b) falsely holds himself out as a cyber inspector;

commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars or imprisonment for a term not exceeding one year or both a fine and

61.(1) A cyber inspector may:

(a) monitor and inspect any web site or activity or an information system in the public domain and report any unlawful activity to the appropriate

(b) in respect of a cryptography service provider-

(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act,

(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;

(c) in respect of an authentication service provider:

(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of

(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Ministry,

(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act;

(d) in respect of a critical information system administration, perform an audit as provided for in section 49.

(2) A police officer may apply for assistance from a cyber inspector to assist in an

62.(1) A cyber inspector may, in the performance of his functions, at any reasonable time and without prior notice, on the authority of a warrant issued in terms of section 63 (1), enter any premises or access an information system that has a bearing on an

(a) search the premises or the information system;

(b) search any person on the premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

(c) take extracts from, or make copies of, any book, document or record that is on or in the premises or information system that has a bearing on the

(d) demand the production and inspect relevant licences and registration certificates as provided in any law;

(e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;

(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is or has been used in connection with any offence on which the investigation is

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information systems;

(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to believe the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide him with such reasonable technical assistance as he may require for the purposes of

(i) make inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based have been

(2) A person who refuses to cooperate or hinders a person conducting a lawful search and seizure in terms of this section commits an offence and is liable to pay a fine not exceeding five thousand dollars or a term of imprisonment not exceeding one year or

63.(1) A cyber inspector may obtain a warrant pursuant to section 41 of the Criminal

(2) For the purposes of subsection (1), a warrant may be issued where:

(a) an offence under this Act has been committed within the State; or

(b) the subject of an investigation is either–

(i) a citizen or ordinarily resident in the State, or

(ii) resent in the State at the time when the warrant is applied for; or

(c) information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and shall:

(a) identify the premises or information system that may be entered and

(b) specify which act may be performed thereunder by the cyber inspector to

(4) A warrant to enter and search premises under this Part may be executed only during the day, unless the judicial officer, who issues it authorises that it may be executed

PART X
INFORMATION SYSTEMS AND COMPUTER RELATED CRIMES

64. In this Part, unless the contrary intention appears:

"access" includes the action of a person who, after taking note of any data, becomes aware of the fact that he is not authorised to access that data and still continues to access that data,

"electronic data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of other article or device;

"electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by a wire, radio, computer, electromagnetic, photo-electric or photo-optical

"electronic mail" means the transmission of information or communication by the use of the internet, a computer, a facsimile machine, a pager, a cellular telephone or other electronic means sent to a person identified by a unique address or address numbers and received by that person;

(a) a public or private entity that provides to users of its services the ability to communicate by means of an information system;

(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 the chain of

(c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.

65. This Part applies to an act done or an omission made:

(a) in Saint Vincent and the Grenadines;

(b) on a ship or air craft registered in Saint Vincent and the Grenadines;

(c) by a national of Saint Vincent and the Grenadines;

(d) by a national of Saint Vincent and the Grenadines outside the territory of Saint Vincent and the Grenadines, if the person's conduct would also constitute an offence under a law of the country where the offence was committed.

66. A person who intentionally, without lawful excuse or justification, accesses the whole or any part of an information system commits an offence and is liable on conviction on indictment to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding two years.

67.(1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:

(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;

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

commits an offence and is liable on conviction on indictment to a fine not exceeding thirty thousand dollars or a term of imprisonment not exceeding four years or to both a

(2) Subsection (1) applies whether the person's act is of temporary or permanent

68.(1) A person who intentionally or recklessly, without lawful excuse or

(a) hinders or interfers with the functioning of an information system; or

(b) hinders or interferes with a person who is lawfully using or operating an information system;

commits an offence and is liable on conviction on indictment to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding ten years or both.

(2) In subsection (1) "hinder" in relation to an information system, includes:

(a) cutting the electricity supply to an information system;

(b) causing electromagnetic interference to an information system;

(c) corrupting a computer system by any means; or

(d) inputting, deleting or altering data.

69. Person who intentionally without lawful excuse or justification intercepts by

(a) any non-public transmission to, from or within an information system; or

(b) electromagnetic emissions from an information system that are carrying

commits an offence and is liable on conviction on indictment to a fine not exceeding fifteen thousand dollars or to a term of imprisonment not exceeding one year or to both a

70.(1) A person commits an offence if the person:

(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise

(i) a device, including a computer programme, that is designed or adapted for the purpose of contravening section 66, 67, 68, or 69,

(ii) a password, access code or similar data by which the whole or any part of an information system is capable of being accessed, with the intent that it be used by any person for contravening section 64, 65, 66, or 67; or

(b) has an item mentioned in sub-paragraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of contravening section 64, 65, 66, or 67.

(2) A person found guilty of an offence under this section is liable on conviction on indictment to a fine not exceeding three thousand dollars or to a term of imprisonment not exceeding twelve months, or to both a fine and imprisonment.

71.(1) A person who intentionally, does any of the following acts:

(a) publishes child pornography through an information system;

(b) produces child pornography for the purpose of its publication through an information system;

or

(c) possesses child pornography in an information system or on an electronic data storage medium,

commits an offence and is liable on conviction on indictment:

(d) in the case of an individual, to a term of imprisonment not exceeding fifteen years or to a term of imprisonment not exceeding ten years or to both a fine and imprisonment;

(e) in the case of a corporation to a fine not exceeding twenty-five thousand

(2) It is a defence to a charge of an offence under subsection (1) (a) or (1) (c) if the person establishes that the child pornography was for a bona fide scientific, research, medical or law enforcement purpose.

(3) In this section:

"child pornography" includes material that visually depicts–

(a) a minor engaged in sexually explicit conduct;

(b) a person who appears to be a minor engaged in sexually explicit conduct or

(c) realistic images representing a minor engaged in sexually explicit conduct

"publish" includes:

(a) 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;

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) 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).

72. A person who fraudulently causes loss of property to another person by:

(a) any input, access, alteration, deleting or suppression of data;

(b) any interference with the functioning of an information system;

with intent to procure for himself or another person an advantage, commits an offence and is liable upon conviction on indictment to a fine not exceeding ten thousand dollars or a term of imprisonment not exceeding five years or to both a fine and imprisonment.

73. A person who:

(a) in an electronic mail or communication uses any words or language threatening to inflict bodily harm to any person or to any member of that person's family or damage to the property of any person;

(b) uses electronic mail or communication, whether or not conversation ensues, for the purpose of abusing, annoying, threatening terrifying, harassing or embarrassing any person;

(c) uses electronic mail or communication to knowingly make any false statement concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct with the intent to abuse, annoy, threaten, terrify, harass or embarrass;

commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or a term of imprisonment not exceeding five years or to both a fine and imprisonment.

PART XI PROCEDURAL POWERS

74. In this Part:

"thing" includes:

(a) an information system or part of an information system; and

(b) another information system if–

(i) data from that information system is available to the first information system being searched, and

(ii) there are reasonable grounds for believing that the information data sought is stored in the other information system;

(c) a data storage medium.

"seize" includes:

(a) make and retain a copy of data, including by using on-site equipment;

(b) render inaccessible, or remove, data in the accessed information system;

(c) take a printout of output of data.

75.(1) If a judicial officer is satisfied on the basis of evidence on oath that there are reasonable grounds to believe that there may be data or in a place or, a thing:

(a) material that may constitute evidence in proving an offence; or

(b) material that has been acquired by a person as a result of an offence;

the judicial officer may issue a warrant authorising a police officer to enter the place to search and seize the data or thing.

76.(1) A person who is in possession or control of an electronic data storage medium or information system that is the subject of a search under section 75 must permit, and assist if required, the person making the search to:

(a) access and use an information system or electronic data storage medium to search any data available to or in the system;

(b) obtain and copy that data;

(c) use equipment to make copies; and

(d) obtain an intelligible output from an information system in a plain text format that can be ready by a person.

(2) A person who fails without lawful excuse or justification to permit a person to search or a person in making a search commits an offence and is liable on summary

(a) in the case of an individual, to a fine not exceeding five thousand dollars or a term of imprisonment not exceeding two years or to both a fine and

(b) in the case of a corporation, to a fine not exceeding fifty thousand dollars.

(3) In this section "assist" includes:

(a) providing passwords;

(b) providing encryption keys;

(c) making available any other information necessary to access an information

77.(1) If an information system or computer data has been removed or rendered inaccessible following a search or a seizure under section 73, the person who made the search must, 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 the list to:

(i) the occupier of the premises, or

(ii) the person in control of the information system.

(2) Subject to sub-section (3), on request, a police officer or another authorized

(a) permit a person who had the custody or control of the information system, or someone acting on the person's behalf to access and copy data on the

(b) give the person a copy of the data.

(3) The police officer or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or

(a) would constitute a criminal offence;

(b) would prejudice,

(i) the investigation in connection with which the search was carried out,

(ii) another ongoing investigation, or any criminal proceedings that are pending or that maybe brought in relation to any of those investigations.

78.(1) If a judicial officer is satisfied on the basis of an application by a police officer that specified data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judicial officer may

(a) a person in Saint Vincent and the Grenadines in control of an information system produce from the system specified data or a printout or other intelligible output of that data;

(b) a service provider in Saint Vincent and the Grenadines produce information about persons who subscribe to or otherwise use the

(2) Where any material to which a criminal investigation relates consists of data stored in an electronic data storage medium, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

79. If a judicial officer is satisfied on the basis of an ex parte application by a police officer for the purpose of a criminal investigation or criminal proceedings, the judicial officer may order that a person in control of the information system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

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

80.(1) If a police officer is satisfied that:

(a) data stored in an information system is reasonably required for the purposes of a criminal investigation; and

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

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

(2) The period may be extended beyond 7 days if, on an ex parte application, a judicial officer authorizes an extension for a further specified period of time.

81. If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judicial officer may:

(a) order a service provider whose service is available in Saint Vincent and the Grenadines through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of data associated with specified communications transmitted by means of an information system;

(b) authorize a police officer to collect or record that data through application

82. If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request

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

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

(2) If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that traffic data is reasonably required for the purposes of a criminal investigation, the judicial officer may authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

83. In proceedings for an offence against a law of Saint Vincent and the Grenadines,

(a) it is alleged that an offence of interfering with an information system has been committed; and

(b) evidence has been generated from that information system;

does not of itself prevent that evidence from being admitted.

84.(1) A service provider who without lawful authority discloses:

(a) the fact that an order under section 76, 77, 78, 79, 80 and 81 has been

(b) anything done under the order; or

(c) any data collected or recorded under the order,

commits an offence and is liable on summary conviction to a fine not exceeding twelve

(2) A service provider is not liable under a civil or criminal law of Saint Vincent and the Grenadines for the disclosure of any data or other information that he discloses under sections 76, 77, 78, 79, 80 and 81.

85. An offence under sections 66, 67, 68, 69 or 72 of this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

PART XII
GENERAL LAW

86. This Act does not affect criminal or civil liability in terms of the common law.

87. The Minister may make Regulations:

(a) to designate an entity as a public body;

(b) to provide that electronic signatures for specified purposes shall be reliable as appropriate for those purposes;

(c) to provide that electronic signatures for specified purposes shall be created by specified means;

(d) to provide formats by which information may be communicated electronically, whether or not there exist prescribed non-electronic forms.

(e) to exclude classes of transactions, documents, or rules of law from the application of this Act;

(f) for any other purpose for the more effective achievement of the objects of Passed in the House of Assembly this day of 2007.

Passed in the House of Assembly this day of 2007.

Clerk of the House of Assembly

OBJECTS AND REASONS

The object of this Bill is to eliminate legal barriers to the effective use of electronic communications; to promote the harmonisation of legal rules on electronic communications across national boundaries; to facilitate the appropriate use of electronic transactions; to promote business and community confidence in electronic transactions, to enable business and community to use electronic communications in their transactions with government and to combat electronic related crime and to facilitate the collection of electronic evidence: In order to embrace technology we must seek to make it as comfortable to do business in that context as it is now with paper and ink. We must also make it safe to do business in that context. The aim of this Bill is to achieve both objectives.

Hon. Jerrol Thompson
Minister of Telecommunications, Science, Technology and Industry

Annex 3E:

TRINIDAD AND TOBAGO EVIDENCE ACT
Chapter 7:02
Act *4 of 1848
Amended by

*12 of 1855
*12 of 1898
*23 of 1905
7 of 1912
31 of 1918
29 of 1925
12 of 1942
39 of 1947
20 of 1953
7 of 1955
16 of 1973
52 of 1976
36 of 1978
45 of 1979
**24 of 1981
2 of 1983
27 of 1986
2 of 1990
12 of 1991
6 of 1993
3 of 1994
11 of 1996
28 of 1996
12 of 1999
**27 of 2000

ARRANGEMENT OF SECTIONS

Annex 3E

Annex 3E

PART VII – GENERAL AND MISCELLANEOUS

FIRST SCHEDULE – *(Repealed by Act No. 28 of 1996)*.

SECOND SCHEDULE.

THIRD SCHEDULE.

NOTES.

FOOTNOTTES.

Annex 3E

Chapter 7:02
EVIDENCE ACT

An Act Relating to the Law of Evidence.

[14th September 1905]
[15th June 1855]
[22nd June 1898]

1. This Act may be cited as the Evidence Act.

PART I
GENERAL

2. Whenever any question arises in any action, suit, information, or other proceeding in or before any Court of Justice, or before any person having by law or by consent of parties authority to hear, receive, and examine evidence touching the admissibility or the sufficiency of any evidence, or the competency or obligation of any witness to give evidence, or the swearing of any witness, or the form of oath or of affirmation to be used by any witness, or the admissibility of any question put to any witness, or the admissibility or sufficiency of any document, writing, matter, or thing tendered in evidence, every such question shall be decided according to the law in force in England on 30th August 1962.

3. A Court shall take judicial notice of any statutory instrument made under a written law of Trinidad and Tobago if the statutory instrument has been published in the Gazette or in the Revised Edition of the Laws of Trinidad and Tobago.

4. The written laws of the legislature of any Commonwealth territory may be proved by copies thereof purporting to be printed by the authority of the legislature or the Government of that country.

5. A party producing a witness shall not be allowed to impeach his credit by general evidence of bad character, but he may, in case the witness in the opinion of the Judge proves adverse, contradict him by other evidence, or by leave of the Judge, prove that he had made at other times a statement inconsistent with his present testimony; but before such last-mentioned proof can be given, the circumstances of the supposed statement, sufficient to designate the particular occasion, must be mentioned to the witness, and he must be asked whether or not he has made such statement.

6. If a witness, upon cross-examination as to a former statement made by him relative to the subject matter of the indictment or proceeding and inconsistent with his present testimony, does not distinctly admit that he did make the statement, proof may be given that he did in fact make it; but before such proof is given, the circumstances of the supposed statement, sufficient to designate the particular occasion, shall be mentioned to the witness, and he shall be asked whether or not he made the statement.

7. A witness may be cross-examined as to previous statements made by him in writing, or reduced into writing, relative to the subject matter of the indictment or proceeding without the writing being shown to him; but if it is intended to contradict the witness by the writing, his attention must, before such contradictory proof is given, be called to those parts of the writing which are to be used for the purpose of so contradicting him; but the Judge, at any time during the trial, may require the production of the writing for his inspection, and may make such use of it for the purposes of the trial as he thinks fit.

8. A witness may be questioned as to whether he has been convicted of any indictable offence, and upon being so questioned, if he either denies or does not admit the fact, or refuses to answer, the cross-examining party may prove the conviction; and a certificate containing the substance and effect only (omitting the formal part) of the indictment and conviction for such offence, purporting to be signed by the Registrar or Clerk of the Court, or other officer having the custody of the records of the Court where the offender was convicted, or by the deputy of such Clerk or officer, is, upon proof of the identity of the person, sufficient evidence of the conviction, without proof of the signature or official character of the person appearing to have signed the same.

9. It is not necessary to prove by the attesting witness any instrument to the validity of which attestation is not requisite, and the instrument may be proved as if there had been no attesting witness.

10. Comparison of a disputed writing with any writing proved to the satisfaction of the Judge to be genuine is permitted to be made by witnesses; and such writing, and the evidence of witnesses respecting it, may be submitted to the Court and jury as evidence of the genuineness or otherwise of the writing in dispute.

11. This Part shall apply to all Courts of Justice, criminal as well as all others, and to all persons having, by law or by consent of parties, authority to hear, receive, and examine evidence.

12. ***(Repealed by Act No. 28 of 1996).***

PART II
EVIDENCE IN CRIMINAL CASES

13.(1) Every person charged is a competent witness for the defence at every stage of the proceedings, whether the person so charged is charged solely or jointly with any other person; but–

(a) a person so charged shall not be called as a witness in pursuance of this section except upon his own application;

(b) the failure of any person charged with an offence, to give evidence shall not be made the subject of any comment by the prosecution;

(c) ***(Repealed by Act No. 28 of 1996).***

(2) A person charged and being a witness in pursuance of this section may be asked any question in cross-examination, notwithstanding that it would tend to criminate him, as to the offence charged.

(3) A person charged and called as a witness in pursuance of this section shall not be asked, and if asked shall not be required to answer, any question tending to show that he has committed or been convicted of or been charged with any offence other than that wherewith he is then charged, or is of bad character, unless–

(a) the proof that he has committed or been convicted of such other offence is admissible evidence to show that he is guilty of the offence wherewith he is then charged; or

(b) he has personally or by his advocate asked questions of the witnesses for the prosecution with a view to establish his own good character, or has given evidence of his good character, or the nature or conduct of the defence is such as to involve imputations on the character of the prosecutor or the witnesses for the prosecution or the victim who is deceased or otherwise incapable of giving evidence of the alleged crime; or

(c) he has given evidence against any other person charged with the same offence.

(4) A person called as a witness in pursuance of this section shall, unless otherwise ordered by the Court, give his evidence from the witness box or other place from which the other witnesses give their evidence.

(5)

(6)

13A.(1) Subject to this Act and the Children Act, every person is competent and compellable to give evidence.

(2) A person who is incapable of understanding that he is under an obligation to give truthful evidence is not competent to give evidence.

(3) Where in the opinion of the Court a person is incapable of understanding and of communicating a reply to a question and where that incapacity cannot be readily overcome for the purposes of the trial, that person is deemed incompetent to give evidence.

13B.(1) Subject to subsections (2) and (3), where a person is charged on indictment, he shall not be entitled to make a statement without being sworn, and accordingly if he gives evidence he shall do so on oath and be liable to cross-examination.

(2) Nothing in subsection (1) shall–

(a) affect the right of a person charged, if not represented by an Attorney-at-law, to address the Court or jury otherwise than on oath on any matter on which, if he were so represented, such attorney-at-law could address the Court or jury on his behalf; or

(b) prevent him from making a statement without being sworn, if–

(i) the statement is one which he is by law required to make personally; or

(ii) the statement is made by way of mitigation before the Court passes sentence upon him.

(3) Nothing in this section shall apply to a trial which began before the commencement of this section.

14.(1) In this section–

“statement” includes any representation of fact, whether made in words or otherwise; “document” includes any device by means of which information is recorded or stored; and

“business” includes every kind of business, profession, occupation, calling, operation or activity, whether carried on for profit or otherwise.

(2) In any criminal proceeding where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, on production of the document, be admissible as evidence of that fact if–

(a) the document is, or forms part of, a record relating to any trade or business and compiled, in the course of that trade or business, from information supplied (whether directly or indirectly) by persons who have, or may reasonably be supposed to have, personal knowledge of the matters dealt with in the information they supply; and

(b) the person who supplied the information recorded in the statement in question is dead, or beyond the seas, or unfit by reason of his bodily or mental condition to attend as a witness, or cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which has elapsed since he supplied the information and to all the circumstances) to have any recollection of the matters dealt with in the information he supplied.

(3) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of this section, the Court may draw any reasonable inference from the form or content of the document in which the statement is contained, and may, in deciding whether or not a person is fit to attend as a witness, act on a certificate purporting to be a certificate of a registered medical practitioner.

(4) In determining the weight, if any, to be attached to a statement admissible as evidence by virtue of this section regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement, and, in particular, to the question whether or not the person who supplied the information recorded in the statement did so contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not that person, or any person concerned with making or keeping the record containing the statement, had any incentive to conceal or misrepresent the facts.

(5) Nothing in this section affects the admissibility of any evidence that would be admissible apart from this section, or makes admissible any statement or document that is privileged.

14A.(1) Subject to subsection (2), in any criminal proceedings a photograph of any object may be admitted in evidence as prima facie proof of the identity of that object, provided that the photograph is supported by a certificate signed by the photographer before a Justice of the Peace authenticating the photograph as being a true image of the object aforesaid.

(2) The photographer shall be required to give evidence of the procedure adopted by him to produce the photograph.

14B.(1) In any criminal proceedings, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein if it is shown that–

(a) there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

(b) at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and

(c) any relevant conditions specified in Rules of Court are satisfied.

(2) Provision may be made by Rules of Court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section, such information concerning the statement as may be required by the Rules shall be provided in such form and at such times as may be so required.

(3) In any proceedings where it is desired to give a statement in evidence in accordance with subsection (1), a certificate–

(a) identifying the document containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

(c) dealing with any of the matters mentioned in subsection (1); and

(d) signed by a person occupying a responsible position in relation to the operation of the computer,

shall be evidence of anything stated in such certificate, and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(4) Notwithstanding subsection (3), a Court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.

(5) Any person who in a certificate tendered under subsection (3), makes a statement which he knows to be false or does not believe to be true is guilty of an offence and liable–

(a) on summary conviction to a fine of three thousand dollars and to imprisonment for six months;

(b) on conviction on indictment to a fine of ten thousand dollars and to imprisonment for two years.

(6) In estimating the weight, if any, to be attached to a statement admitted pursuant to this section regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular–

(a) to the question whether or not the information reproduced in or derived from the statement was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

(b) to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced, had any incentive to conceal or misrepresent the facts.

(7) For the purposes of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or, with or without human intervention, by means of any appropriate equipment.

(8) For the purpose of deciding whether or not a document is admissible in evidence by virtue of subsection (1) the Court may draw any reasonable inference–

(a) from the circumstances in which the statement was made or otherwise came into being; or

(b) from any other circumstance, including the form and contents of the document in which the statement is contained.

14C. Where a statement contained in a document is admissible in criminal proceedings, it may be proved–

(a) by the production of that document; or

(b) by the production of a copy of that document, or of the material part of it, whether or not that document is still in existence,

and authenticated in such manner as the Court may approve; and it is immaterial for the purposes of this section the extent to which the original or a copy thereof may have been reproduced.

14D.(1) In any criminal proceeding or inquest, any record kept by a Government expert relating to anything submitted to him for examination, analysis or report shall be prima facie evidence of the particulars recorded therein.

(2) For the purposes of subsection (1) "Government expert" has the same meaning as that expression bears in section 19(4).

14E. The Rules Committee established by the Supreme Court of Judicature Act, may, subject to negative resolution of Parliament, make Rules necessary for the purposes of this Part.

15.(1) Where the only witness to the facts of the case called by the defence is the person charged, he shall be called as a witness immediately after the close of the evidence for the prosecution.

(2) In cases where the right of reply depends upon the question whether evidence has been called for the defence, the fact that the person charged has been called as a witness shall not of itself confer on the prosecution the right of reply.

15A.(1) Any requirement at common law whereby at a trial on indictment it is obligatory for the Court to give the jury a warning about convicting the accused on the uncorroborated evidence of a person because that person is–

(a) an alleged accomplice of the accused; or

(b) a person in respect of whom it is alleged that a sexual offence under the Sexual Offences Act, has been committed,

is abrogated.

(2) Any requirement that is applicable at the summary trial of a person for an offence and corresponds to the requirement mentioned in subsection (1) is abrogated.

(3) Nothing in this section shall prevent a Judge from exercising his discretion to advise a jury of the need for corroboration.

(4) Nothing in this section applies to any trial on indictment or to any proceedings before a Magistrate's Court which began before the commencement of this section.

PART III
EVIDENCE IN PARTICULAR CASES

16. The parties to any action for breach of promise of marriage are competent to give evidence in such action; but no plaintiff in any action for breach of promise of marriage may recover a verdict unless his or her testimony is corroborated by some other material evidence in support of such promise.

17. The parties to any proceeding instituted in consequence of adultery, and their husbands and wives are competent to give evidence in such proceeding, but no witness in any proceeding, whether a party to the suit or not, shall be liable to be asked or bound to answer any question tending to show that he or she has been guilty of adultery, unless such witness has already given evidence in the same proceeding in disproof of his or her alleged adultery.

18. The parties to any information or proceeding in the High Court for the recovery of any penalty for the breach of any law relating to the revenue are competent to give evidence in any such information or proceeding.

19.(1) A document purporting to have affixed, impressed, or subscribed thereon or thereto the seal and signature of any diplomatic agent of Trinidad and Tobago in any foreign country, or any consular officer of Trinidad and Tobago in any foreign place, in testimony of any oath, affidavit, or act administered, taken, or done by or before any such person shall be admitted in evidence in any Court of Trinidad and Tobago without proof of his seal or signature or of his official character.

(1A) Where a document is attested to in a foreign country and purports to have affixed, impressed, or subscribed thereon the seal and signature of a notary public, a commissioner for oaths or where there is no such office any other person duly authorised by statute to administer oaths or to take statutory declarations in that country, such document shall be admitted in any Court in Trinidad and Tobago without proof of the seal or signature or due authorisation and such document shall be as effectual as if administered, taken or done by or before any lawful authority in Trinidad and Tobago.

(2) In any criminal proceeding any document purporting to be a certificate or report under the hand of a Government expert on any matter or thing which has been submitted to him for examination, analysis or report is admissible as evidence of the facts stated in it without proof

of the signature or appointment of the Government expert, unless the Court, acting ex proprio motu or at the request of a party to the proceeding requires the expert to be called as a witness. The Court is not bound to require the attendance of the expert as a witness if the Court is of opinion that the request for such attendance is made for the purpose of vexation, delay or defeating the ends of justice.

(2A) Where medical evidence is contained in a report signed by–

(a) a District Medical Officer, and the evidence–

(i) relates to a fatality; and

(ii) is being led in criminal proceedings or in an inquest; or

(b) a registered medical practitioner and the evidence does not relate to a fatality, the report shall be admitted as if it were the report of a Government expert within the meaning of this section.

(3) In any inquest held by a Coroner any such certificate or report is likewise admissible as evidence of the facts stated in it unless the Coroner requires the expert to be called as a witness.

(4) In this section–

"Government expert" means the following public officers:

(a) Senior Pathologist;

(b) Pathologist;

(c) Government Chemist; (d) Armourer;

**(e)* Forensic Document Examiner;

(f) Forensic Biologist;

(g) Scientific Examiner (Motor Vehicle);

(h) the holder of any other office or any other suitably qualified and experienced person declared by the President by Notification published in the Gazette to be an officer or person to which this section applies;

"report" includes a post mortem report.

PART IV
EVIDENCE RELATING TO BIRTHS, DEATHS AND MARRIAGES

20.(1) A certified copy of an entry in any register of births, deaths, or marriages purporting to bear the signature of the person having legal custody of such register, or of some person legally authorised to sign such copy at the time of its issue, and authenticated as provided below is, in the case of any register kept at any place in Commonwealth countries subject to all just exceptions, prima facie evidence for all purposes of the fact of the birth or death or the legal solemnisation of the marriage thereby certified.

(2) A certified copy shall bear the signature of a person describing himself as holding some office, benefice, or position entitling him to the custody of the register, or to sign such copy at the time of so certifying, and the authentication of such signature shall be under the hand and seal of a Notary Public, or under the hand of the Registrar General, or Superintendent Registrar of Births and Deaths, or Registrar of Marriages of the Commonwealth country within which such certificate purports to have been issued, or under the hand of a member of the High Court or Supreme Court of such Commonwealth country, or under the seal of a Court of civil jurisdiction in the district in which the certified copy was issued.

(3) At the preliminary examination in respect of or at any trial for any indictable offence, where it becomes necessary either for the prosecution or the defence to establish the fact of any birth, death, or marriage in any Commonwealth country, the person charged, or the wife or husband of the person charged, may give evidence of the identity of any person with any person named in the certificate; but nothing contained in this Act shall be construed to make it compulsory on any person accused, or on his or her wife or husband, to give any such evidence if he or she is unwilling to do so.

(4) A birth, death, or marriage in the United Kingdom and the Republic of Ireland or in Trinidad and Tobago shall, saving all just exceptions, be proved in the manner provided in this section, any written law to the contrary notwithstanding.

PART V
DOCUMENTARY EVIDENCE IN CERTAIN CASES

21. In this Part –

"Government Printer" means and includes any printer purporting to be the printer authorised to print the Acts and other documents of the Government;

"document" means and includes proclamations, orders, bye-laws, rules, regulations, warrants, circulars, lists, assessment rolls, minutes, certificates, notices, requisitions, letters, decrees, and all other records and writings whatsoever of a public character pertaining to the several departments of the Government in the first column of the Second Schedule;

"bankers' books" means and includes ledgers, day books, cash books, account books, and all other books used in the ordinary business of a bank;

"legal proceeding" means any civil or criminal proceeding or enquiry in which evidence is or may be given before any Court of Justice, Judge, Magistrate or Justice, Arbitrator, Commissioner or person or persons authorised by the Supreme Court to take evidence;

"Judge" means a Judge of the Supreme Court, or of a Petty Civil Court; "bank" and "banker" means and includes –

(a) any person or persons, partnership or company, carrying on the business of bankers in Trinidad and Tobago, or the manager;

(b) any person or persons, partnership or company, who may hereafter carry on the business of bankers in Trinidad and Tobago and who hereafter, under the authority of any Act may establish a banking association in Trinidad and Tobago, or the manager;

(c) the Post Office Savings Bank established under the Post Office Savings Bank Act. In the case of the said Savings Bank, "banker" means the Postmaster General.

22.(1) Every document issued–

(a) by the President;

(b) under the authority of the President;

(c) by or under the authority of any department of the Government or officer mentioned in the first column of the Second Schedule; or

(d) being a record in any such department of the Government,

may be received in evidence in all Courts of Justice, and in all legal proceedings whatsoever, in every case in which the original document would be admissible in evidence in all or any of the following modes:

(i) by production of a copy of the Gazette purporting to contain the document;

(ii) by production of a copy of the document purporting to be printed by the Government Printer;

(iii) by production (in the case of any document issued by the President or under the authority of the President) of a copy or extract purporting to be certified by the Minister, Secretary to the Cabinet or any Permanent Secretary; and

(iv) by production (in the case of any document issued by or under the authority of any of the departments or officer, or being a record in any such department of the Government) of a copy or extract purporting to be certified to be true by the person or persons specified in the second column of the said Second Schedule in connection with such department or officer.

Any copy or extract made in pursuance of this Part may be in print or in writing, or partly in print and partly in writing.

No proof shall be required of the handwriting or official position of any person certifying in pursuance of this Part to the truth of any copy of or extract from any document.

(2) In this section "Minister" means the Minister responsible for the subject matter in respect of which the document was issued and "Permanent Secretary" means the Permanent Secretary to the Minister.

23. No officer of any of the several public departments specified in the first column of the Second Schedule is, in any legal proceedings to which the State or he is not a party, compellable to produce any document the contents of which can be proved under this Act or to appear as a witness to prove the matters, transactions, and things recorded in it unless by order of a Judge made for special cause.

24. Any person who prints any enactment or document which falsely purports to have been printed by the Government Printer, or by the authority of the legislation or the Government of any Commonwealth territory or tenders in evidence any document which falsely purports to have been so printed knowing that the same was not so printed is liable to imprisonment for five years.

25. Section 22 shall be deemed to be in addition to and not in derogation of any powers of proving documents given by any Act or law for the time being in force in Trinidad and Tobago.

26. Subject to this Act, a copy of any entry in a banker's book shall, in all legal proceedings be received as prima facie evidence of such entry, and of the matters, transactions, and accounts therein recorded.

27.(1) A copy of an entry in a banker's book shall not be received in evidence under this Act unless it is first proved that the book was, at the time of the making of the entry, one of the ordinary books of the bank, and that the entry was made in the usual and ordinary course of business, and that the book is in the custody or control of the bank.

(2) Such proof may be given by the manager or accountant of the bank, and in the case of the Post Office Savings Bank by the Postmaster General or any person authorised by him.

(3) Such proof may be given orally, or by affidavit sworn, or statutory declaration made, before any Commissioner or person authorised to take affidavits or statutory declarations.

28. A copy of an entry in a banker's book shall not be received in evidence under this Act unless it be further proved that the copy has been examined with the original entry and is correct; such proof shall be given by some person who has examined the copy with the original entry, and may be given either orally, or by an affidavit sworn, or statutory declaration made, before any Commissioner or person authorised to take affidavits or statutory declarations.

29. The manager or accountant of a bank, and in the case of the Post Office Savings Bank the Postmaster General and any person employed in connection with the Post Office Savings Bank, are not, in any legal proceeding to which the bank is not a party, compellable to produce any

banker's book, the contents of which can be proved under this Act or to appear as a witness to prove the matters, transactions, and accounts recorded in it, unless by order of a Judge made for special cause.

30. On the application of any party to a legal proceeding, a Court or Judge may order that the party be at liberty to inspect and take copies of any entries in a banker's book for any of the purposes of the proceedings. An order under this section may be made either with or without summoning the bank or any other party, and shall be served on the bank three clear days, exclusive of Sundays and public holidays, before it is to be obeyed, unless the Court or Judge otherwise directs.

31.(1) There shall be paid to and taken by the officers of the departments in the Second Schedule mentioned, except the Registrar General's department, the following fees, that is to say:

For every copy of any document, for every 90 words... ... ...

For a certificate of correctness of such copy ...

All fees under this Act shall be paid to the Comptroller of Accounts.

(2) There shall be paid to the Commissioner of Police for information relating to a road traffic accident a fee of fifty dollars.

(3) The fees specified in the Third Schedule shall be paid by private clients in respect of services provided by the Trinidad and Tobago Forensic Science Centre.

(4) The Minister may by Order amend the Third Schedule.

32.(1) In any proceeding, whether civil or criminal, an instrument as to the validity of which attestation is requisite may, instead of being proved by an attesting witness be proved in the manner in which it might be proved if no attesting witness were alive.

(2) In this section "proceedings" includes an arbitration or reference whether under any written law or not.

(3) Nothing in this section shall apply to the proof of Wills or other testamentary documents.

33. In any proceedings, whether civil or criminal, there shall, in the case of documents proved, or purporting, to be not less than twenty years old be made any presumption which immediately before 1st September 1938 would have been made in the case of a document of like character proved, or purporting, to be not less than thirty years old.

34. Nothing in section 32 or 33 shall prejudice the admissibility of any evidence which would, apart from the provisions of those sections, be admissible.

PART VI
EVIDENCE IN CIVIL PROCEEDINGS

35.(1) In this Part–

"civil proceedings" includes, in addition to civil proceedings in any of the ordinary Courts of Law–

(a) civil proceedings before any other tribunal, being proceedings in relation to which the strict rules of evidence apply; and

(b) an arbitration or reference, whether under a written law or not,

but does not include civil proceedings in relation to which the strict rules of evidence do not apply; "computer" has the meaning assigned by section 40;

"Court" does not include a Court-martial, and, in relation to an arbitration or reference, means the arbitrator or umpire and, in relation to proceedings before a tribunal (not being one of the ordinary Courts of law), means the tribunal;

"document" includes, in addition to a document in writing–

(a) any map, plan, graph or drawing;

(b) any photograph;

(c) any disc, tape, sound track or other device in which sounds or other data, not being visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as mentioned above) of being reproduced therefrom;

"film" includes a microfilm;

"legal proceedings" includes an arbitration or reference, whether under a written law or not; "statement" includes any representation of fact, whether made in words or otherwise.

(2) In this Part any reference to a copy of a document includes–

(a) in the case of a document falling within paragraph (c) but not (d) of the definition of "document" in subsection (1), a transcript of the sounds or other data embodied therein;

(b) in the case of a document falling within paragraph (d) but not (c) of that definition, a reproduction or still reproduction of the image or images embodied therein, whether enlarged or not;

(c) in the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and

(d) in the case of a document not falling within the said paragraph (d) of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not,

and any reference to a copy of the material part of a document shall be construed accordingly.

(3) For the purposes of the application of this Part in relation to any such civil proceedings as are mentioned in subsection (1), any Rules of Court made for the purposes of this Act under sections 77 and 78 of the Supreme Court of Judicature Act, shall (except in so far as their operation is excluded by agreement) apply, subject to such modifications as may be appropriate, in like manner as they apply in relation to civil proceedings in the High Court of Justice.

(4) If any question arises as to what are, for the purposes of any such civil proceedings as are mentioned in subsection (1), the appropriate modifications of any such rule of Court as is mentioned in subsection (3), that question shall, in default of agreement, be determined by the tribunal or the arbitrator or umpire, as the case may be.

(5) Any reference in this Part to any other written law includes a reference thereto as applied, by or under any other written law.

(6) Nothing in this Part prejudices the operation of any written law which provides (in whatever words) that any answer or evidence given by a person in specified circumstances is not admissible in evidence against him or some other person in any proceedings or class of proceedings (however described).

(7) In subsection (6) the reference to giving evidence is a reference to giving evidence in any manner, whether by furnishing information, making discovery, producing documents or otherwise.

(8) Nothing in this Part prejudices–

(a) any power of a Court, in any legal proceeding, to exclude evidence (whether by preventing questions from being put or otherwise) at its discretion; or

(b) the operation of any agreement (whenever made) between the parties to any legal proceedings as to the evidence which is to be admissible (whether generally or for any particular purpose) in those proceedings.

(9) Where, by reason of any defect of speech or hearing from which he is suffering, a person called as a witness in any legal proceeding gives his evidence in writing or by signs, that evidence is to be treated for the purposes of this Part as being given orally.

36.(1) In any civil proceedings a statement other than one made by a person while giving oral evidence in those proceedings is admissible as evidence of any fact stated therein to the extent that it is so admissible by virtue of any provision of this Part or by virtue of any other statutory provision or by agreement of the parties, but not otherwise.

(2) In this section "statutory provision" means any provision contained in, or in an instrument made under, this or any other Act including any Act passed after the commencement of the Evidence (Amendment) Act 1973 (that is, 15th November 1973).

37.(1) In any civil proceedings a statement made, whether orally or in a document or otherwise, by any person, whether called as a witness in those proceedings or not, shall, subject to this section and to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

(2) Where in any civil proceedings a party desiring to give a statement in evidence by virtue of this section has called or intends to call as a witness in the proceedings the person by whom the statement was made, the statement–

(a) shall not be given in evidence by virtue of this section on behalf of that party without the leave of the Court; and

(b) without prejudice to paragraph (a), shall not be given in evidence by virtue of this section on behalf of that party before the conclusion of the examination-in-chief of the person by whom it was made, except–

(i) where before that person is called the Court allows evidence of the making of the statement to be given on behalf of that party by some other person; or

(ii) in so far as the Court allows the person by whom the statement was made to narrate it in the course of his examination-in-chief on the ground that to prevent him from doing so would adversely affect the intelligibility of his evidence.

(3) Where in any civil proceedings a statement which was made otherwise than in a document is admissible by virtue of this section, no evidence other than direct oral evidence by the person who made the statement or any person who heard or otherwise perceived it being made shall be admissible for the purpose of proving it, but so however, that if the statement in question was made by a person while giving oral evidence in some other legal proceedings (whether civil or criminal), it may be proved in any manner authorised by the Court.

38.(1) Where in any civil proceedings–

(a) a previous inconsistent or contradictory statement made by a person called as a witness in those proceedings is proved by virtue of section 5, 6 or 7;

(b) a previous statement made by a person called as aforesaid is proved for the purpose of rebutting a suggestion that his evidence has been fabricated,

that statement shall by virtue of this subsection be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

(2) Nothing in this Part shall affect any of the rules of law relating to the circumstances in which, where a person called as a witness in any civil proceedings is cross-examined on a document used by him to refresh his memory, that document may be made evidence in those proceedings; and where a document or any part of a document is received in evidence in any such proceedings by virtue of any such rule of law, any statement made in that document or

part by the person using the document to refresh his memory shall by virtue of this subsection be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible.

39.(1) Without prejudice to section 40, in any civil proceedings a statement contained in a document shall, subject to this section and to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if the document is, or forms part of, a record compiled by a person acting under a duty from information which was supplied by a person (whether acting under a duty or not) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with in that information and which, if not supplied by that person to the compiler of the record, directly, was supplied by him to the compiler, of the record indirectly through one or more intermediaries, each acting under a duty.

(2) Where in any civil proceedings a party desiring to give a statement in evidence by virtue of this section has called or intends to call as a witness in the proceedings the person who originally supplied the information from which the record containing the statement was compiled, the statement–

(a) shall not be given in evidence by virtue of this section on behalf of that party without the leave of the Court; and

(b) without prejudice to paragraph (a), shall not, without the leave of the Court, be given in evidence by virtue of this section on behalf of that party before the conclusion of the examination-in-chief of the person who originally supplied the said information.

(3) Any reference in this section to a person acting under a duty includes a reference to a person acting in the course of any trade, business, profession or other occupation in which he is engaged or employed or for the purposes of any paid or unpaid office held by him.

40.(1) In any civil proceedings a statement contained in a document produced by a computer shall, subject to Rules of Court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown that the conditions mentioned in subsection (2) are satisfied in relation to the statement and computer in question.

(2) The said conditions are–

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

(3) Where over a period the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2)(a) was regularly performed by computers, whether–

(a) by a combination of computers operating over that period;

(b) by different computers operating in succession over that period;

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this Part as constituting a single computer; and references in this Part to a computer shall be construed accordingly.

(4) In any civil proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say–

(a) identifying the document containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this Part–

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) where, in the course of activities carried on by any individual or body, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

(6) Subject to subsection (3) in this Part "computer" means any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process.

41.(1) Without prejudice to the generality of section 22, where in any civil proceedings a statement contained in a document is proposed to be given in evidence by virtue of section 37, 39 or 40 it may, subject to any Rules of Court, be proved by the production of that document or (whether or not that document is still in existence) by the production of a copy of that document, or of the material part thereof, authenticated in such manner as the Court may approve.

(2) For the purpose of deciding whether or not a statement is admissible in evidence by virtue of section 37, 39 or 40 the Court may draw any reasonable inference from the circumstances in which the statement was made or otherwise came into being or from any other circumstances, including, in the case of a statement contained in a document the form and contents of that document.

(3) In estimating the weight, if any, to be attached to a statement admissible in evidence by virtue of section 37, 38, 39 or 40 regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular–

(a) in the case of a statement falling within section 37(1) or 38(1) or (2), to the question whether or not the statement was made contemporaneously with the occurrence or

existence of the facts stated, and to the question whether or not the maker of the statement had any incentive to conceal or misrepresent the facts;

(b) in the case of a statement falling within section 39(1), to the question whether or not the person who originally supplied the information from which the record containing the statement was compiled did so contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not that person, or any person concerned with compiling or keeping the record containing the statement, had any incentive to conceal or misrepresent the facts; and

(c) in the case of a statement falling within section 40(1) to the question whether or not the information which the information contained in the statement reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied thereto, contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.

(4) For the purpose of any written law or rule of law or practice requiring evidence to be corroborated or regulating the manner in which uncorroborated evidence is to be treated–

(a) a statement which is admissible in evidence by virtue of section 37 or 38 shall not be capable of corroborating evidence given by the maker of the statement; and

(b) a statement which is admissible in evidence by virtue of section 8 shall not be capable of corroborating evidence given by the person who originally supplied the information from which the record containing the statement was compiled.

(5) Any person who, in a certificate tendered in evidence in civil proceedings by virtue of section 40(4), wilfully makes a statement material in those proceedings which he knows to be false or does not believe to be true is liable on conviction on indictment to a fine and to imprisonment for two years.

42.(1) Subject to Rules of Court, where in any civil proceedings a statement made by a person who is not called as a witness in those proceedings is given in evidence by virtue of section 37–

(a) any evidence which, if that person had been so called, would be admissible for the purpose of destroying or supporting his credibility as a witness shall be admissible for that purpose in those proceedings; and

(b) evidence tending to prove that, whether before or after he made that statement, that person made (whether orally or in a document or otherwise) another statement inconsistent therewith shall be admissible for the purpose of showing that that person has contradicted himself.

(2) Nothing in subsection (1) shall enable evidence to be given of any matter of which, if the person in question had been called as a witness and had denied that matter in cross-examination, evidence could not have been adduced by the cross-examining party.

(3) Subsection (1) shall apply in relation to a statement given in evidence by virtue of section 39 as it applies in relation to a statement given in evidence by virtue of section 37, except that references to the person who made the statement and to his making the statement shall be construed, respectively, as references to the person who originally supplied the information from which the record containing the statement was compiled and to his supplying that information.

(4) Section 38(1) shall apply to any statement proved by virtue of subsection (l)(b) as it applies to a previous inconsistent or contradictory statement made by a person called as a witness which is proved as mentioned in paragraph (a) of the said section 38(1).

Annex 3E

43.(1) Provision shall be made by Rules of Court as to the procedure which, subject to any exceptions provided for in the Rules, must be followed and the other conditions which, subject as aforesaid, must be fulfilled before a statement can be given in evidence in civil proceedings by virtue of section 37, 39 or 40.

(2) Rules of Court made in pursuance of subsection (1) shall in particular, subject to such exceptions (if any) as may be provided for in the Rules–

(a) require a party to any civil proceedings who desires to give in evidence any such statement as is mentioned in that subsection to give to every other party to the proceedings such notice of his desire to do so and such particulars of or relating to the statement as may be specified in the Rules, including particulars of such one or more of the persons connected with the making or recording of the statement or, in the case of a statement falling within section 37(1), such one or more of the persons concerned as mentioned in section 41(3)(c) as the Rules may in any case require; and

(b) enable any party who receives such notice as aforesaid by counter-notice to require any person of whom particulars were given with the notice to be called as a witness in the proceedings; unless that person is dead, or beyond the seas, or unfit by reason of his bodily or mental condition to attend as a witness, or cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which has elapsed since he was connected or concerned as aforesaid and to all the circumstances) to have any recollection of matters relevant to the accuracy or otherwise of the statement.

(3) Rules of Court made in pursuance of subsection (1)–

(a) may confer on the Court in any civil proceedings a discretion to allow a statement falling within section 37(1), 39(1) or 40(1) to be given in evidence notwithstanding that any requirement of the rules affecting the admissibility of that statement has not been complied with; except in pursuance of paragraph (b), Rules of Court may not confer on the Court a discretion to exclude such a statement where the requirements of the rules affecting its admissibility have been complied with;

(b) may confer on the Court power, where a party to any civil proceedings has given notice that he desires to give in evidence–

(i) a statement falling within section 37(1) that was made by a person, whether orally or in a document, in the course of giving evidence in some other legal proceedings (whether civil or criminal); or

(ii) a statement falling within section 39(1) that is contained in a record of any direct oral evidence given in some other legal proceedings (whether civil or criminal), to give directions on the application of any party to the proceedings as to whether, and if so on what conditions, the party desiring to give the statement in evidence will be permitted to do so (where applicable) as to the manner in which that statement and any other evidence given in those other proceedings is to be proved; and

(c) may make different provision for different circumstances, and in particular may make different provisions with respect to statements falling within sections 37(1), 39(1) and 40(1), respectively,

and any discretion conferred on the Court by Rules of Court made in accordance with this section may be either a general discretion or a discretion exercisable only in such circumstances as may be specified in the Rules.

(4) Rules of Court may make provision for preventing a party to any civil proceedings (subject to any exceptions provided for in the Rules) from adducing in relation to a person who is not called as a witness in those proceedings any evidence that could otherwise be adduced by him

by virtue of section 42, unless that party has in pursuance of the Rules given in respect of that person such a counter-notice as is mentioned in subsection (2)(b).

(5) In deciding for the purposes of any Rules of Court made in pursuance of this section whether or not a person is fit to attend as a witness, a Court may act on a certificate purporting to be a certificate of a registered medical practitioner.

(6) Nothing in the foregoing provisions of this section shall prejudice the generality of section 76 of the Supreme Court of Judicature Act, or any other written law conferring power to make Rules of Court; and nothing in any enactment restricting the matters with respect to which Rules of Court may be made shall prejudice the making of Rules of Court with respect to any matter mentioned in the foregoing provisions of this section or the operation of any Rules of Court made with respect to any such matter.

44.(1) In any civil proceedings a statement which, if this Part had not been passed, would by virtue of any rule of law mentioned in subsection (2) have been admissible as evidence of any fact stated therein shall be admissible as evidence of that fact by virtue of this subsection.

(2) The rules of law referred to in subsection (1) are the following, that is to say any rule of law:

(a) whereby in any civil proceedings an admission adverse to a party to the proceedings, whether made by that party or by another person, may be given in evidence against that party for the purpose of proving any fact stated in the admission;

(b) whereby in any civil proceedings published works dealing with matters of a public nature (for example, histories, scientific works, dictionaries and maps) are admissible as evidence of facts of a public nature stated therein;

(c) whereby in any civil proceedings public documents (for example, public registers, and returns made under public authority with respect to matters of public interest) are admissible as evidence of facts stated therein; or

(d) whereby in any civil proceedings records (for example, the records of certain Courts, treaties, State grants, pardons and commissions) are admissible as evidence of facts stated therein.

In this subsection "admission" includes any representation of fact, whether made in words or otherwise.

(3) In any civil proceedings a statement which tends to establish reputation or family tradition with respect to any matter and which, if this Part had not been passed, would have been admissible in evidence by virtue of any rule of law mentioned in subsection (4)–

(a) shall be admissible in evidence by virtue of this paragraph in so far as it is not capable of being rendered admissible under section 37 or 39; and

(b) if given in evidence under this Act (whether by virtue of paragraph (a) or otherwise) shall by virtue of this paragraph be admissible as evidence of the matter reputed or handed down,

and, without prejudice to paragraph (b), reputation shall for the purposes of this Act be treated as a fact and not as a statement or multiplicity of statements dealing with the matter reputed.

(4) The rules of law referred to in subsection (3) are the following, that is to say any rule of law:

(a) whereby in any civil proceedings evidence of a person's reputation is admissible for the purpose of establishing his good or bad character;

(b) whereby in any civil proceedings involving a question of pedigree or in which the existence of a marriage is in issue, evidence of reputation or family tradition is admissible for the purpose of proving or disproving pedigree or the existence of the marriage, as the case may be; or

(c) whereby in any civil proceedings evidence of reputation or family tradition is admissible for the purpose of proving or disproving the existence of any public or general right or of identifying any person or thing.

(5) It is hereby declared that in so far as any statement is admissible in any civil proceedings by virtue of subsection (1) or (3)(a), it may be given in evidence of those proceedings notwithstanding anything in sections 37 to 42 or in any Rules of Court made in pursuance of section 43.

(6) The words in which any rules of law mentioned in subsection (2) or (4) is there described are intended only to identify the rule in question and shall not be construed as altering that rule in any way.

45.(1) In any civil proceedings–

(a) the fact that a person has been found guilty of, or to have committed, adultery in any matrimonial proceedings; and

(b) the fact that a person has been adjudged to be the father of a child in affiliation proceedings before any Court in Trinidad and Tobago,

shall [subject to subsection (3)] be admissible in evidence for the purpose of proving, where to do so is relevant to any issue in those civil proceedings, that he committed the adultery to which the finding relates, or, as the case may be, is (or was) the father of that child, whether or not he offered any defence to the allegation of adultery or paternity and whether or not he is a party to the civil proceedings; but no finding or adjudication other than a subsisting one shall be admissible in evidence by virtue of this section.

(2) In any civil proceedings in which by virtue of this section a person is proved to have been found guilty of, or to have committed, adultery as mentioned in subsection (l)(a) or to have been adjudged to be the father of a child as mentioned in subsection (l)(b)–

(a) he shall be taken to have committed the adultery to which the finding relates or, as the case may be, to be (or have been) the father of that child, unless the contrary is proved; and

(b) without prejudice to the reception of any other admissible evidence for the purpose of identifying the facts on which the finding or adjudication was based, the contents of any document which was before the Court or which contains any pronouncement of the Court, in the matrimonial or affiliation proceedings in question shall be admissible in evidence for that purpose.

(3) Nothing in this section shall prejudice the operation of any enactment whereby a finding of fact in any matrimonial or affiliation proceedings is for the purposes of any other proceedings made conclusive evidence of any fact.

46.(1) The following rules of law are hereby abrogated except in relation to criminal proceedings, that is to say:

(a) the rule whereby, in any legal proceedings, a person cannot be compelled to answer any question or produce any document or thing if to do so would tend to expose him to a forfeiture; and

(b) the rule whereby, in any legal proceedings, a person other than a party to the proceedings cannot be compelled to produce any Deed or other document relating to his title to any land.

(2) The rule of law whereby, in any civil proceedings, a party to the proceedings cannot be compelled to produce any document relating solely to his own case and in no way tending to impeach that case or support the case of any opposing party is hereby abrogated.

47. This Act binds the State.

Annex 3F

THE BAHAMAS No. 4 of 2033

An Act to Provide for the Legal Recognition of Electronic Writing, Electronic Contracts, Electronic Signatures and Original Information in Electronic Form in Relation to Commercial and Other Transactions and to Provide for the Facilitation of Electronic Transactions and Related Matters. [Date of Assent: 11th April, 2003]
Enacted by the Parliament of The Bahamas.

PART I
PRELIMINARY

1. Short title and commencement.

(1) This Act may be cited as the Electronic Communications and Transactions Act, 2003.

(2) This Act shall come into operation on such day as the Minister may, by notice published in the Gazette, appoint.

2. Interpretation. In this Act –

"addressee" in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication;

"consumer" means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes;

"e-commerce service provider" means a person who uses electronic means in providing goods and services;

"electronic" means relating to technology and having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

"electronic authentication" means any procedure employed for the purpose of verifying that an electronic communication is that of the originator and that it has not been altered during transmission;

"electronic agent" means a program, or other electronic or automated means that is used independently to initiate or respond to electronic communications or performances in whole or in part without review by an individual;

"electronic communication" means information which is communicated, processed, recorded, displayed, created, stored, generated, received or transmitted by electronic means;

"electronic signature" means any letters, characters, numbers, sound, process or symbols in electronic form attached to, or logically associated with information that is used by a signatory to indicate his intention to be bound by the content of that information;

"host" means a person who provides a service that consists of the storage in electronic form of information provided by another person;

"information" includes data, text, documents, images, sounds, codes, computer programs, software and databases;

Annex 3F

"information processing system" means an electronic system for creating, generating, sending, receiving, recording, storing, displaying, or otherwise processing information;

"intermediary" with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives or stores either temporary or permanently that electronic communication or provides related services with respect to that electronic communication;

"Minister" means the Minister with responsibility for Electronic Commerce;

"originator" in relation to an electronic communication, means a person by whom, or on whose behalf, the electronic communication purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that electronic communication;

"prescribed" means prescribed by regulations under section 24;

"public body" means any Ministry, agency, board, commission or other body of the Government and includes an entity or body established by law, or by arrangement of the Government or a Minister of the Government for a non-commercial public service purpose;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

"security procedure" means a procedure, established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, communication or performance is that of a particular person or for detecting changes or errors in content of an electronic communication;

"signed" or "signature" includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic methods;

"transaction" means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including the sale, lease, exchange, licensing, or other disposition of personal property, including goods and Intangibles, interest in real property, services, or any combination of the foregoing.

2. Crown to be bound.

(1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act obliges any public body to generate, send, receive, store or otherwise process any record by electronic means, but the Minister may, by notice published in the Gazette, indicate that a public body may receive and process electronic communications relating to such matters as may be specified in the notice.

3. Exclusions.

Part II shall not apply to any rule of law requiring writing or signatures for the following–

(a) the creation, execution, amendment, variation or revocation of–

(i) a will or testamentary instrument; or

(ii) a trust;

(b) the conveyance of real property or the transfer of any interest in real property;

(c) court orders or notices, or official court documents required to be executed in connection with court proceedings;

(d) enduring powers of attorney to the extent that they concern the financial affairs or personal care of an individual;

(e) all other deeds and documents described in section 3 of the Registration of Records Act, not otherwise expressly provided for under this subsection.

4. Autonomy of parties.

(1) Nothing in this Act shall–

(a) require any person to use or accept electronic communications, electronic signatures, or electronic contracts; or

(b) prohibit any person engaging in a transaction through the use of electronic means from–

(i) varying by agreement any provision relating to legal recognition and functional equivalency of electronic communications, signatures, and contracts specified in Part II; or.

(ii) establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

(2) A transaction which has been conducted using electronic means shall not be denied legal effect, validity, or enforceability because of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

5. Consumer consent to electronic communications.

Notwithstanding section 7, if a statutory or legal requirement exists for a record to be provided in writing to a consumer, such requirement for writing shall be satisfied by an electronic communication only if–

(a) the consumer has expressly consented to such use and has not withdrawn his consent; and

(b) prior to consenting, the consumer is provided with a clear and conspicuous statement informing the consumer–

(i) about the right to have the record provided in non-electric form;

(ii) about the right to withdraw consent to have the record provided in electronic form and of any conditions, consequences or fees in the event of such withdrawal;

(iii) whether the consent applies only to the particular transaction which gave rise to the obligation to provide the record, or to identified categories of records that may be provided during the course of the parties' relationship;

(iv) of the hardware and software requirements for access to, and retention of, the relevant electronic record;

(v) of the procedures for withdrawal of consent and to update information needed to contact the consumer electronically; and

(vi) of the procedures, after consent has been given, for obtaining a paper copy of the electronic record and any fee to be charged in connection therewith.

PART II
LEGAL RECOGNITION AND FUNCTIONAL EQUIVALENCY OF ELECTRONIC COMMUNICATIONS, SIGNATURES, CONTRACTS AND RELATED MATTERS

6. Legal recognition of electronic communications.

An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is–

(a) in electronic form; or

(b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication.

7. Writing.

(1) Where information is required bylaw either to be in writing or is described as being written, such requirement or description is met by an electronic communication if the information contained in the electronic communication is accessible to, and is capable of retention by, the intended recipient.

(2) Subsection (1) shall apply whether the requirement for the information to be in writing is in the form of an obligation or the law provides consequences if it is not in writing.

8. Signature.

(1) Where the law requires the signature of a person, that requirement is met in relation to an electronic communication if a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic communication.

(2) Subsection (1) shall apply whether the requirement for a signature is in the form of an obligation or the law provides consequences for the absence of a signature.

(3) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic communication is that of such party.

9. Original form.

(1) Where information is required by law to be presented or retained in its original form, that requirement is met by an electronic communication if –

(a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its / final form as an electronic communication or otherwise; and

(b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

(2) Subsection (1) shall apply whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of subsection (1)(a) –

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

10. Retention of electronic communications.

(1) Where certain documents, records or information are required by law to be retained, that requirement is met by retaining electronic communications if the following conditions are satisfied–

(a) the information contained in the electronic communication is accessible so as to be usable for subsequent reference;

(b) the electronic communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received is retained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) shall not extend to any information the sole purpose of which is to enable the message to be sent or received.

Annex 3F

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out in subsection (1)(a), (b) and (c) are met.

(4) Nothing in this section shall preclude any public body from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of such public body.

11. Admissibility and evidential weight of electronic communications.

(1) In any legal proceedings, nothing in the' rules of evidence shall apply so as to deny the admissibility of an electronic communication in evidence solely on the ground that it is in electronic form.

(2) Information in the form of an electronic communication will be given due evidential weight and in assessing the evidential weight of an electronic communication, regard shall be had to–

(a) the reliability of the manner in which the electronic communication was generated, stored or transmitted;

(b) the reliability of the manner in which the integrity of the information was maintained;

(c) the manner in which the originator was identified; and

(d) any other relevant factor. (3) No. 15 1996.

(3) This section shall not affect the application of sections 61 and 67 of the Evidence Act (which relates to the admissibility of documents produced by computers).

12. Formation and validity of contracts.

In the context of formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic communications.

13. Attribution of electronic communications.

(1) An electronic communication is attributable to a person if the electronic communication resulted from the action of the person, acting in person, by his agent, or by his electronic agent device.

(2) Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic communication was attributable.

(3) An addressee is not entitled to regard the electronic communication received as being what the originator intended to send where the addressee knew or ought reasonably to have known, had he exercised reasonable care or used an agreed procedure, that the transmission resulted in any error in the electronic communication as received.

(4) Nothing in this section affects the law of agency or the law on the formation of contracts.

14. Acknowledgement of receipt of electronic communications.

(1) Where the originator of an electronic communication has stated that the electronic communication is conditional upon receipt of an acknowledgement–

(a) the electronic communication is to be treated as though it had never been sent until the acknowledgement is received;

(b) if there is no agreement between the originator and the addressee as to the particular form or method of the acknowledgement to be given, the addressee may give an acknowledgement by any means of communication automated or otherwise or by any conduct that is reasonably sufficient to indicate to the originator that the electronic communication has been received.

(2) Where the originator indicates that receipt of an electronic communication is required to be acknowledged but has not stated that the electronic communication is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator –

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the electronic communication as though it had never been sent or exercise any other rights the originator may have.

(3) Where the received acknowledgement states that the related electronic communication met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(4) Except in so far as it relates to the sending or receipt of the electronic record, this section is not intended to deal with the legal consequences that may flow either from that electronic communication or from the acknowledgement of its receipt.

15. Notarisation.

Where any statutory or legal requirement exists for a document to-be notarised, verified, or made under oath, that requirement is met if the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

16. Delivery, etc.

(1) Where information is required by law to be delivered, dispatched, given or sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic communication provided that the originator of the electronic communication states that the receipt of the electronic communication is to be acknowledged and the addressee has acknowledged its receipt.

(2) Subsection (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

(3) Subject to section 5, the dispatch of an electronic communication occurs when it enters an information processing system outside the control of the originator.

(4) Subject to section 5, the time of receipt of an electronic communication is determined as follows –

(a) where the addressee has designated an information processing system for the purpose of receiving electronic communications, receipt occurs –

(i) at the time when the electronic communication enters the designated information processing system; or

(ii) if the electronic communication is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic communication comes to the attention of the addressee;

(b) where the addressee has not designated an information processing system, receipt is deemed to have occurred on the earlier happening of –

(i) the time at which the electronic communication enters an information processing system of the addressee; or

(ii) otherwise comes to the attention of the addressee.

(5) Subsection (4) shall apply notwithstanding that the place where the information processing system is located may be different from the place where the electronic communication is deemed to be received under subsection (6).

(6) Unless otherwise agreed between the originator and the addressee, an electronic communication is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(7) For the purposes of subsection (6) –

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic communication relates or, where there is no such transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

17. Copyright.

(1) The generation of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

(2) The production, by means of an electronic communication, of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

PART III
INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

18. Liability of intermediaries.

(1) An intermediary shall not be subject to any civil or criminal liability in respect of third-party information contained in an electronic communication for which such intermediary is only providing access and he –

(a) has no actual knowledge that the information gives rise to civil or criminal liability;

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or

(c) follows the procedure set out in section 20 if the intermediary–

(i) acquires knowledge that the information gives rise to civil or criminal liability; or

(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary shall not be required to monitor any information contained in an electronic communication in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

(3) Nothing in this section shall relieve an intermediary from complying with any court order, injunction, writ, Ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic communication.

(4) For the purposes of this section –

"provides access", in relation to third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing access;

"third-party information" means information of which the intermediary is not the originator.

19. Procedure for dealing with unlawful, defamatory, etc. information.

(1) If an intermediary has actual knowledge that the information in an electronic communication gives rise to civil or criminal liability, as soon as practicable thereafter the intermediary shall –

(a) remove the information from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the police of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary.

(2) If an intermediary is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic communication ought reasonably to have been known, as soon as practicable thereafter the intermediary shall –

(a) follow the relevant procedure set out in any code of conduct that is applicable to such intermediary under section 21; or

(b) notify the police and the Minister.

(3) Upon being notified in respect of any information under subsection (2), the Minister may direct the intermediary to –

(a) remove the electronic communication from any information processing system within the control of the intermediary; and

(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication.

(4) An intermediary shall not be liable, whether in contract, tort, under statute or pursuant to any other right, to any person, including any person on whose behalf the intermediary provides services in respect of information in an electronic communication, for any action the intermediary takes in good faith in exercise of the powers conferred by, or as directed by the Minister under, this section.

20. Codes of conduct and standards for intermediaries and e-commerce service providers.

(1) If a code of conduct is approved-or a standard is appointed by the Minister under this section to apply to intermediaries or e-commerce service providers, those intermediaries or e-commerce service providers shall comply with such code of conduct or standard.

(2) An intermediary or e-commerce service provider who fails to comply with an approved code of conduct or appointed standard, shall in the first instance be given a written warning by the Minister and the Minister may direct that person to cease and desist or otherwise to correct his practices, and, if that person fails to do so within such period as may be specified in the direction, he commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars and if the offence is a continuing one to a further fine of five hundred dollars for each day the offence continues.

(3) If the Minister is satisfied that a body or organization represents intermediaries or e-commerce service providers, the Minister may, by notice given to the body or organization, request the body or organization to –

(a) develop a code of conduct that applies to intermediaries or e-commerce service providers and that deals with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and

(b) provide a copy of that code of conduct to the Minister within such time as may be specified in the request.

(4) If the Minister is satisfied with the code of conduct provided under subsection (3), the Minister shall approve the code of conduct by notice published in the Gazette and thereupon the code of conduct will apply to intermediaries or e-commerce service providers as the case may be, as may be specified in the notice.

(5) If the Minister is satisfied that –

(a) no body or organization represents intermediaries or e-commerce service providers; or

(b) a body or organization to which notice is given under subsection (3) has not complied with the request of the Minister under that subsection,

the Minister may, by notice published in the Gazette, appoint a standard that applies to intermediaries or e-commerce service providers.

(6) If the Minister has approved a code of conduct or appointed a standard that applies to intermediaries or e-commerce service providers and –

(a) the Minister receives notice from a body or organization representing intermediaries or e-commerce service providers of proposals to amend the code of conduct or standard; or

(b) the Minister no longer considers that the code of conduct or standard is appropriate, the Minister may, by notice published in the Gazette, revoke or amend any existing code of conduct or standard.

(7) References in this section to intermediaries or e-commerce service providers include reference to a particular class of intermediary or e-commerce service provider.

PART IV
E-COMMERCE ADVISORY BOARD

21. E-Commerce Advisory Board.

(1) There shall be a board to be known as the "E-Commerce Advisory Board" for the purpose of providing advice to the Minister on matters connected with the discharge of his functions under this Act and the development of e-commerce and the information and communications technology sector generally.

(2) The Minister shall appoint the members of the Board by notice published in the Gazette.

(3) The Board shall consist of not less than five or more than nine persons appearing to the Minister to be knowledgeable about electronic commerce, information technology, communications, finance education, law or international business.

(4) The Minister shall designate one of the persons appointed a member under subsection (2) to be the chairman of the Board.

(5) The Board shall determine its own procedure.

(6) The persons appointed under subsection (2) shall hold office for such period and on such terms as may be determined by the Minister.

(7) The function of the Board is to advise the Minister on any matter referred to it by the Minister or which, of its own initiative, the Board considers appropriate.

Annex 3F

PART V
GENERAL

22. General provisions as to prosecutions under the Act.

(1) Where a body corporate commits an offence under this Act or regulations made hereunder, every person who at the time of the commission of the offence was a director, officer, general manager, chief executive officer, managing director of the corporation, or a person purporting to act in any such capacity commits the like offence unless he proves that the contravention took place without his consent or that he exercised all due diligence to prevent the commission of the offence.

(2) Unless otherwise expressly provided for under this Act and regulations made pursuant thereto, the penalty for conviction of an offence under this Act shall be –

(a) on summary conviction, to a fine not exceeding three thousand dollars or to imprisonment for twelve months, or to both;

(b) on conviction on information, to a fine not exceeding one hundred thousand dollars or to imprisonment for ten years, or to both.

23. Regulations.

(1) The Minister may make regulations–

(a) for the purpose of establishing how electronic documents may be signed and verified;

(b) respecting the use, import and export of encryption technology, encryption programs, or other encryption products;

(c) for the purpose of authorising, prohibiting or regulating the use of the .bs domain name or any successor domain name for The Bahamas;

(d) prescribing for the purposes of the registration of the .bs domain name or any successor domain name for The Bahamas –

(i) designated registration authorities; (ii) the form of registration;

(iii) the period when registration stays in force;

(iv) the manner, the terms and the period for renewal of registration;

(v) the circumstances and manner in which registration may be granted, renewed or refused by the registration authorities;

(vi) the appeal process;

(vii) the fees to be paid on the grant or renewal of registration and the time and manner they are to be paid; and

(viii) such other matters relating to the registration of domain names;

(e) generally for the better carrying out of the provisions of this Act.

(2) Ch. 2.

Notwithstanding section 25(e) of the Interpretation and General Clauses Act, a person who contravenes or fails to comply with a regulation made pursuant to subsection (1) is liable on summary conviction to a fine not exceeding one thousand dollars.

(3) Regulations made under this section are subject to the affirmative resolution of Parliament.

(4) The term “affirmative resolution” as used in this section means that the regulations shall not come into operation unless and until affirmed by a resolution of each House of Parliament.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013