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

Electronic Evidence: Model Policy Guidelines & Legislative Texts

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:

Model Policy Guidelines & Legislative Texts

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.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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.

In response to both the challenges and the opportunities from 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 (@CP-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 Mr. Gilberto Martíns de Almeida and Ms. Pricilla Banner. The draft document was then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information Society Issues, held in Saint Lucia on 8-12 March 2010 and in Barbados on 23-26 August 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Mr. Martíns de Almeida addressing, *inter alia*, the points raised at the second workshop.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries, representatives from the ministries of justice and legal affairs and other public sector bodies, regulators, academia, civil society, operators, and regional organizations, for their hard work and commitment in producing the contents of this report. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The contributions from the Caribbean Community (CARICOM) Secretariat 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 a document such as this, 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 Morain, 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 Division (CYB). Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

Table of contents

Introduction

1.1. HIPCAR Project – Aims and Beneficiaries

The HIPCAR project[1] was officially launched in the Caribbean by the International Telecommunication Union (ITU) and the European Commission (EC) in December 2008, in close collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU). The HIPCAR project is part of a global ITU-EC-ACP project encompassing also sub-Saharan Africa and the Pacific.

HIPCAR's objective is to assist CARICOM/ACP/CARIFORUM[2] countries in the Caribbean to harmonize their information and communication technology (ICT) policies, legislation and regulatory procedures so as to create an enabling environment for ICT development and connectivity, thus facilitating market integration, fostering investment in improved ICT capabilities and services, and enhancing the protection of ICT consumers' interests across the region. The project's ultimate aim is to enhance competitiveness and socio-economic and cultural development in the Caribbean region through ICTs.

In accordance with Article 67 of the Revised Treaty of Chaguaramas, HIPCAR can be seen as an integral part of the region's efforts to develop the CARICOM Single Market & Economy (CSME) through the progressive liberalization of its ICT services sector. The project also supports the CARICOM Connectivity Agenda and the region's commitments to the World Summit on the Information Society (WSIS), the World Trade Organization's General Agreement on Trade in Services (WTO-GATS) and the Millennium Development Goals (MDGs). It also relates directly to promoting competitiveness and enhanced access to services in the context of treaty commitments such as the CARIFORUM states' Economic Partnership Agreement with the European Union (EU-EPA).

The beneficiary countries of the HIPCAR project include Antigua and Barbuda, The Bahamas, Barbados, Belize, The Commonwealth of Dominica, the Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

1.2. Project Steering Committee and Working Groups

HIPCAR has established a project Steering Committee to provide it with the necessary guidance and oversight. Members of the Steering Committee include representatives of Caribbean Community (CARICOM) Secretariat, Caribbean Telecommunications Union (CTU), Eastern Caribbean Telecommunications Authority (ECTEL), Caribbean Association of National Telecommunication Organisations (CANTO), Caribbean ICT Virtual Community (CIVIC), and International Telecommunication Union (ITU).

---

1 The full title of the HIPCAR Project is: "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures". HIPCAR is part of a global ITU-EC-ACP project carried out with the funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). It is implemented by the ITU in collaboration with the Caribbean Telecommunications Union (CTU) and with the involvement of other organizations in the region. (see www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

2 The CARIFORUM is a regional organisation of fifteen independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Christopher and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago). These states are all signatories to the ACP–EC Conventions.

In order to ensure stakeholder input and relevance to each country, HIPCAR Working Groups have also been established with members designated by the country governments – including specialists from ICT agencies, justice and legal affairs and other public sector bodies, national regulators, country ICT focal points and persons responsible for developing national legislation. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The Working Groups also include representatives from relevant regional bodies (CARICOM Secretariat, CTU, ECTEL and CANTO) and observers from other interested entities in the region (e.g. civil society, the private sector, operators, academia, etc.).

The Working Groups have been responsible for covering the following two work areas:

1. *ICT Policy and Legislative Framework on Information Society Issues*, dealing with six sub-areas: e-commerce (transactions and evidence), privacy & data protection, interception of communications, cybercrime, and access to public information (freedom of information).
2. *ICT Policy and Legislative Framework on Telecommunications*, dealing with three sub-areas: universal access/service, interconnection, and licensing in a convergent environment.

The reports of the Working Groups published in this series of documents are structured around these two main work areas.

1.3. Project Implementation and Content

The project's activities were initiated through a Project Launch Roundtable organized in Grenada, on 15-16 December 2008. To date, all of the HIPCAR beneficiary countries – with the exception Haiti – along with the project's partner regional organizations, regulators, operators, academia, and civil society have participated actively in HIPCAR events including – in addition to the project launch in Grenada – regional workshops in Trinidad & Tobago, St. Lucia, St. Kitts and Nevis, Suriname and Barbados.

The project's substantive activities are being led by teams of regional and international experts working in collaboration with the Working Group members, focusing on the two work areas mentioned above.

During *Stage I* of the project – just completed – HIPCAR has:

1. Undertaken assessments of the existing legislation of beneficiary countries as compared to international best practice and in the context of harmonization across the region; and
2. Drawn up model policy guidelines and model legislative texts in the above work areas, from which national ICT policies and national ICT legislation/regulations can be developed.

It is intended that these proposals shall be validated or endorsed by CARICOM/CTU and country authorities in the region as a basis for the next phase of the project.

Stage II of the HIPCAR project aims to provide interested beneficiary countries with assistance in transposing the above models into national ICT policies and legislation tailored to their specific requirements, circumstances and priorities. HIPCAR has set aside funds to be able to respond to these countries' requests for technical assistance – including capacity building – required for this purpose.

1.4. Overview of the Six HIPCAR Model Policy Guidelines and Legislative Texts Dealing with Information Society Issues

Countries worldwide as well as in the Caribbean are looking for ways to develop legal frameworks addressing the needs of information societies with a view to leveraging the growing ubiquity of the World Wide Web as a channel for service delivery, ensuring a safe environment and the processing power of information systems to increase business efficiency and effectiveness.

Introduction

The Information Society is based on the premise of access to information and services and utilizing automated processing systems to enhance service delivery to markets and persons anywhere in the world. For both users and businesses the information society in general and the availability of information and communication technology (ICT) offers unique opportunities. As the core imperatives of commerce remain unchanged, the ready transmission of this commercial information creates opportunities for enhanced business relationships. This ease of exchange of commercial information introduces new paradigms: firstly, where information is used to support transactions related to physical goods and traditional services; and secondly, where information itself is the key commodity traded.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe). Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements.

However, the transformation process is going along with challenges as the existing legal framework does not necessary cover the specific demands of a rapidly changing technical environment. In cases where information supports trade in traditional goods and services, there needs to be clarity in how traditional commercial assumptions are effected; and in the instance where information is the commodity traded, there needs to be protection of the creator/ owner of the commodity. In both instances, there needs to be rationalization of how malfeasance is detected, prosecuted and concluded in a reality of trans-border transactions based on an intangible product.

The Six Inter-related Model Frameworks

The HIPCAR project has developed six (6) inter-related model frameworks that provide a comprehensive legal framework to address the above mentioned changing environment of information societies by guiding and supporting the establishment of harmonized legislation in the HIPCAR beneficiary countries.

Firstly a legal framework was developed to protect the right of users in a changing environment and thereby among other aspects ensuring consumer and investor confidence in regulatory certainty and protection of privacy, HIPCAR model legislative texts were developed to deal with considerations relating to: **Access to Public Information (Freedom of Information)** – geared to encouraging the appropriate culture of transparency in regulatory affairs to the benefit of all stakeholders; and **Privacy and Data Protection** – aimed at ensuring the protection of privacy and personal information to the satisfaction of the individual. This latter framework is focused on appropriate confidentiality practices within both the public and private sectors.

Secondly, in order to facilitate harmonization of laws with regard to the default expectations and legal validity of contract-formation practices, a HIPCAR model legislative text for **Electronic Commerce (Transactions)**, including electronic signatures was developed. This framework is geared to provide for the equivalence of paper and electronic documents and contracts and for the foundation of undertaking commerce in cyber-space. A legislative text dealing with **Electronic Commerce (Evidence)** – the companion to the Electronic Commerce (Transactions) framework, was added to regulate legal evidence in both civil and criminal proceedings.

To ensure that grave violations of the confidentiality, integrity and availability of ICT and data can be investigated by law enforcement, model legislative texts were developed to harmonise legislation in the field of criminal law and criminal procedural law. The legislative text on **Cybercrime** defines offences, investigation instruments and the criminal liability of key actors. A legislative text dealing with the **Interception of Electronic Communications** establishes an appropriate framework that prohibits the illegal interception of communication and defines a narrow window that enables law enforcement to lawfully intercept of communication if certain clearly defined conditions are fulfilled.

Developing the Model Legislative Texts

The model legislative texts were developed by taking into account key elements of international trends as well as legal traditions and best practices from the region. This process was undertaken to ensure that to the frameworks optimally meet the realities and requirements of the region of HIPCAR beneficiary countries for which and by which they have been developed. Accordingly, the process involved significant interaction with stakeholders at each stage of development.

The first step in this complex process was an assessment of existing legal frameworks within the region through a review of the laws related to all relevant areas.. In addition to enacted legislation, the review included, where relevant, bills which had been prepared but had yet to complete the process of promulgation. In a second step, international best practices (for example from United Nations, OECD, EU, the Commonwealth, UNCITRAL and CARICOM) as well as advanced national legislation (for example from the UK, Australia, Malta and Brazil, among others) were identified. Those best practices were used as benchmarks.

For each of the six areas, complex legal analyses were drafted that compared the existing legislation in the region with these benchmarks. This comparative law analysis provided a snapshot of the level of advancement in key policy areas within the region. These findings were instructive, demonstrating more advanced development in frameworks relating to Electronic Transactions, Cybercrime (or “Computer Misuse”) and Access to Public Information (Freedom of Information) legislation than evidenced in the other frameworks.

Based upon the results of the comparative law analyses, the regional stakeholders developed baseline policy “building blocks” which – once approved by stakeholders – defined the bases for further policy deliberation and legislative text development. These policy building blocks reaffirmed some common themes and trends found in the international precedents, but also identified particular considerations that would have to be included in the context of a region consisting of sovereign small island developing states. An example of a major situational consideration which impacted deliberations at this and other stages of the process was the question of institutional capacity to facilitate appropriate administration of these new systems.

The policy building blocks were then used to develop customised model legislative texts that meet both international standards and the demand of the HIPCAR beneficiary countries. Each model text was then again evaluated by stakeholders from the perspective of viability and readiness to be translated into regional contexts. As such, the stakeholder group – consisting of a mix of legislative drafters and policy experts from the region – developed texts that best reflect the convergence of international norms with localised considerations. A broad involvement of representatives from almost all 15 HIPCAR beneficiary countries, regulators, operators, regional organizations, civil society and academia ensured that the legislative texts are compatible with the different legal standards in the region. However, it was also recognised that each beneficiary state might have particular preferences with regard to the implementation of certain provisions. Therefore, the model texts also provide optional approaches within the generality of a harmonised framework. This approach aims to facilitate widespread acceptance of the documents and increase the possibility of timely implementation in all beneficiary jurisdictions.

Interaction and Overlapping Coverage of the Model Texts

Due to the nature of the issues under consideration, there are common threads that are reflected by all six frameworks.

In the first instance, consideration should be given to the frameworks that provide for the use of electronic means in communication and the execution of commerce: **Electronic Commerce (Transactions), Electronic Commerce (Evidence), Cybercrime** and **Interception of Communications**. All four frameworks deal with issues related to the treatment of messages transmitted over communications networks, the establishing of appropriate tests to determine the validity of records or documents, and the mainstreaming of systems geared to ensure the equitable treatment of paper-based and electronic material in maltreatment protection, consumer affairs and dispute resolution procedures.

As such, there are several common definitions amongst these frameworks that need to take into account, where necessary, considerations of varying scope of applicability. Common concepts include: "electronic communications network" – which must be aligned to the jurisdiction's existing definition in the prevailing Telecommunications laws; "electronic document" or "electronic record" – which must reflect broad interpretations so as to include for instance audio and video material; and "electronic signatures", "advanced electronic signatures", "certificates", "accredited certificates", "certificate service providers" and "certification authorities" – which all deal with the application of encryption techniques to provide electronic validation of authenticity and the recognition of the technological and economic sector which has developed around the provision of such services.

In this context, **Electronic Commerce (Transactions)** establishes, among other things, the core principles of recognition and attribution necessary for the effectiveness of the other frameworks. Its focus is on defining the fundamental principles which are to be used in determining cases of a civil or commercial nature. This framework is also essential in defining an appropriate market structure and a realistic strategy for sector oversight in the interest of the public and of consumer confidence. Decisions made on the issues related to such an administrative system have a follow-on impact on how electronic signatures are to be procedurally used for evidentiary purposes, and how responsibilities and liabilities defined in the law can be appropriately attributed.

With that presumption of equivalence, this allows the other frameworks to adequately deal with points of departure related to the appropriate treatment of electronic information transfers. The **Cybercrime** framework, for example, defines offences related to the interception of communication, alteration of communication and computer-related fraud. The **Electronic Commerce (Evidence)** framework provides a foundation that introduces electronic evidence as a new category of evidence.

One important common thread linking **e-Transactions** and **Cybercrime** is the determination of the appropriate liability and responsibility of service providers whose services are used in situations of electronically mediated malfeasance. Special attention was paid to the consistency in determining the targeted parties for these relevant sections and ensuring the appropriate application of obligations and the enforcement thereof.

In the case of the frameworks geared to improving regulatory oversight and user confidence, the model texts developed by HIPCAR deal with opposite ends of the same issue: whereas the **Access to Public Information** model deals with encouraging the disclosure of public information with specified exceptions, the **Privacy and Data Protection** model encourages the protection of a subset of that information that would be considered exempted from the former model. Importantly, both these frameworks are geared to encouraging improved document management and record-keeping practices within the public sector and – in the case of the latter framework – some aspects of the private sector as well. It is however notable that – unlike the other four model texts – these frameworks are neither applicable exclusively to the electronic medium nor about creating the enabling framework within which a new media's considerations are transposed over existing procedures. To ensure consistency, frameworks are instead geared to regulating the appropriate management of information resources in both electronic and non-electronic form.

There are a number of sources of structural and logistical overlaps which exist between these two legislative frameworks. Amongst these is in the definition of the key concepts of "public authority" (the persons to whom the frameworks would be applicable), "information", "data" and "document", and the relationship amongst these. Another important form of overlap concerns the appropriate oversight of these frameworks. Both of these frameworks require the establishment of oversight bodies which should be sufficiently independent from outside influence so as to assure the public of the sanctity of their decisions. These independent bodies should also have the capacity to levy fines and/or penalties against parties that undertake activities to frustrate the objectives of either of these frameworks.

In Conclusion

The six HIPCAR model legislative texts provide the project's beneficiary countries with a comprehensive framework to address the most relevant area of regulation with regard to information society issues. They were drafted by reflecting both the most current international standards as well as the demands of small islands developing countries in general and – more specifically – those of HIPCAR's beneficiary countries. The broad involvement of stakeholders from these beneficiary countries in all phases of development of the model legal texts ensures that they can be adopted smoothly and in a timely manner. Although the focus has been on the needs of countries in the Caribbean region, the aforementioned model legislative texts have already been identified as possible guidelines also by certain countries in other regions of the world.

Given the specific and interrelated natures of the HIPCAR model texts, it will be most advantageous for the project's beneficiary countries to develop and introduce legislation based on these models in a coordinated fashion. The Electronic Commerce models (Transactions and Evidence) will function most effectively with the simultaneous development and passage of Cybercrime and Interception of Communications frameworks, as they are so closely related and dependent on each other to address the concerns of robust regulatory development. Similarly, the Access to Public Information and the Privacy and Data Protection frameworks consist of such synergies in administrative frameworks and core skill requirements that simultaneous passage can only strengthen both frameworks in their implementation.

In this way there will be optimal opportunity created to utilise the holistic frameworks that are established in the region.

1.5. This Report

This report deals with Electronic Evidence in e-Commerce, one of the work areas of the Working Group on the ICT Policy and Legislative Framework on Information Society Issues. It includes Model Policy Guidelines and a Model Legislative Text including Explanatory Notes that countries in the Caribbean may wish to use when developing or updating their own national policies and legislation in this area.

Prior to drafting this document, HIPCAR's team of experts – working closely with the above Working Group members – prepared and reviewed an assessment of existing legislation on information society issues in the fifteen HIPCAR beneficiary countries in the region focusing on six areas: Electronic Transactions, Electronic Evidence in e-Commerce, Privacy and Data Protection, Interception of Communications, Cybercrime, and Access to Public Information (Freedom of Information). This assessment took account of accepted international and regional best practices.

This regional assessment – published separately as a companion document to the current report[3] – involved a comparative analysis of current legislation on Electronic Evidence in e-Commerce in the HIPCAR beneficiary countries and the identification of potential gaps in this regard, thus providing the basis for

[3] See "ICT Policy and Legislative Framework on Information Society Issues – Electronic Evidence in e-Commerce: Assessment Report on the Current Situation in the Caribbean" available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

the development of the model policy framework and legislative text presented herein. By reflecting national, regional and international best practices and standards[4] while ensuring compatibility with the legal traditions in the Caribbean, the model documents in this report are aimed at meeting and responding to the specific requirements of the region.

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants, including Mr. Gilberto Martíns de Almeida and Ms. Pricilla Banner. The model legislative text on Electronic Evidence in e-Commerce was developed in three phases: (1) the drafting of an assessment report; (2) the development of model policy guidelines; and (3) the drafting of the model legislative text. The draft document was then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information Society Issues, held in Saint Lucia on 8-12 March 2010 and in Barbados on 23-26 August 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Mr. Martíns de Almeida addressing, *inter alia*, the points raised at the second workshop. The HIPCAR Project Steering Committee and the Project Management Team oversaw the process of developing these documents. This document therefore contains data and information as known in August 2010.

Following this process, the documents were finalized and disseminated to all stakeholders for consideration by the governments of the HIPCAR beneficiary countries.

1.6. The Importance of Effective Policies and Legislation on Electronic Evidence in e-Commerce

Electronic commerce – as well as other contemporary usages of ICTs – relies on the legal admissibility of electronic evidence as a fundamental condition for inspiring the trust required to allow it to flourish. This fact has been acknowledged by the international community, as represented by UNCITRAL's and the Commonwealth's Model Laws on Electronic Evidence, as well as by relevant legislation to this effect implemented in a large number of States.

As a matter of fact, the increasing dangers to the integrity, availability, confidentiality, authenticity and authorship of electronic documents resulting from 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 relating to the judicial admissibility of electronic evidence.

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

Given such opposite trends and possibilities, a balance needs to be provided by regulation conciliating the relevant technical and procedural aspects in order to harness evidence at a 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 the adoption of prevention or risk-reduction measures), and the principle of accreditation (which demands accredited certification of processes, to inspire a greater level of confidence).

[4] As reflected in the ITU's Toolkit for Cybercrime Legislation and Understanding Cybercrime: A Guide for Developing Countries, the Commonwealth Model Law on Electronic Evidence (LMM(02)1), 2002/58/EC Directive, and national approaches both within and outside of the region.

Introduction

Regulating on digital evidence is a task faced with several challenges such as the proportionate protection of privacy rights and of the principle of non self-incrimination. Data retention and encryption are examples of issues where the production of digital evidence lies at the intersection of security and privacy concerns.

The lack of local regulation on digital evidence is a fact well noticed by hackers and other cybercriminals, who target countries less likely to pursue cases based on electronic evidence. Botnet schemes are an example of threats posed to citizens, governments and businesses in countries that do not have specific legislation providing guidance and criteria on admissible investigation, production, gathering, and keeping of digital evidence.

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. 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 2002, the Commonwealth Secretariat made a recommendation to either adopt or adapt its model legislation in this domain across all Commonwealth countries. 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 and new international standards are examples of new issues to be considered.

In the context of this scenario, regulation on electronic evidence must be articulated in conjunction with regulation in areas such as expedited preservation of data, production order, search and seizure proceedings, data retention and others, in order to provide for its required efficacy.

Section I:
Model Policy Guidelines – Electronic Evidence

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Electronic Evidence in e-Commerce.

1. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH NECESSARY COMMON INTERPRETATIONS FOR KEY TERMS ASSOCIATED WITH E-EVIDENCE[5]

- There shall be proper definition on "computer", "device", "computer data", "computer system," "content data", "traffic data", "location data", "document", "electronic record", "electronic document", "electronic signature", "digital signature", and "time-stamping".
- There shall be sufficiently broad wording in the definition of these terms, coupled with a list of illustrative examples.
- There shall be definition on what terminology shall be left for judicial construction within the jurisdiction of each Beneficiary state, and on how to follow-on on such judicial activity to keep statutory definitions and judicial definitions aligned.

2. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH THE NECESSARY FRAMEWORK TO DEFINE THE PUBLIC OR PRIVATE ORIGIN, AND ROLE, OF THE PARTIES IN CHARGE OF COLLECTING AND/OR MANAGING E-EVIDENCE[6]

- There shall be provision in law which states what is the role of "public authorities", Prosecutors, and Police, and, where applicable, "accreditation authority", "certificate service providers", "registrars", "24x7 access", in the collection and/or management of e-evidence.
- There shall be provision establishing that public authorities shall comply with the rules for e-evidence collection and management established in public information security laws or policies (for instance, regarding the limits for use of cryptography, procedures in treating with devices, and other protocols consistent with international best practice for digital forensic investigation.).
- There shall be provisions recognizing co or self-regulation in certain sectors of markets or of activities, especially where digital signatures and the use of other technologies do not offer a reasonable cost/benefit.
- There shall be provisions establishing the principles and areas where admissibility of e-evidence shall be primarily based on procedural standards.
- There shall be provisions for the establishment and enforcement of technical standards designed to foster proper e-evidence collection and/or management.
- Where applicable, there shall be provision establishing the principle of reciprocity for recognition of digital certificates issued in a third party country, under Regional common laws and authority, or not.
- Where applicable, there shall be provision establishing that public authority shall, in certain instances, be extended to private entities provided those entities are designated to act as "e-Notaries" – persons providing third party digital authentication of parties without the adhering to the technical and procedural tests of a registered certificate service providers.
- Where applicable, there shall be definition on what characterizes "notarization" and therefore the extent to which an e-Notaries' functions have rights and the duties legally associated to it.

[5] There should be public campaign with a view to developing awareness on e-evidence, including explanation on key terms, based on the discretion of each Beneficiary state.

[6] There shall be public policy for building skills in the Judiciary so that judges and technical experts are familiar with the use of e-evidence key concepts, terminology, and procedural standards.
There shall be public policy encouraging institutional cooperation for development of applications using e-evidence as a way to permit greater electronic automation of public service.

Section I

3. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE THE LEGAL MANDATES AND THE STANDARDS TO WHICH E-EVIDENCE SHALL BE BOUND

- The law/legal mandate shall define "electronic records system" for the purposes of interpreting this policy.
- The law/legal mandate should be enabling in nature and refrain from being overly prescriptive in its provisions.
- The law/legal mandate shall state that no electronic document shall be denied legal effect for the sole fact of being electronic.
- Where applicable, the law/legal mandate shall define the extent to which procedural standards relating to the collection, management and/or use of electronic records shall base admissibility of electronic documents and the circumstances which shall require technical e-evidence submission.
- The law/legal mandate shall specify the legal grounds of electronic evidence, and clearly extend its admissibility to administrative and judicial activities (including, in civil, commercial, criminal, labour, administrative, and other matters).
- The law/legal mandate shall establish the nature and effects of the legal presumption associated with e-evidence, so as to establish its weight vis-à-vis other kinds of evidence (documental, and others).
- The law/legal mandate shall define and provide for the publication of information on appropriate standards for update, storage, and disposal of e-evidence.
- The law/legal mandate shall make provisions for the duration for keeping data produced, collected, stored and/or managed as e-evidence, which bear equivalence to the usual practices for managing non-electronic evidence.
- The law/legal mandate shall provide for the public sector utilizing means to encourage transparency with regard to available resources and tools which can facilitate the establishment of e-evidence.
- The law/legal mandate shall determine that the collection and management of e-evidence be guided by the objectives of security, efficiency, effectiveness.
- There shall be public policy encouraging institutional cooperation for development of applications using e-evidence as a way to permit greater electronic automation of public service.
- The law/legal mandate shall define guidelines addressing the principle of technological neutrality, so as to provide for flexibility in developing e-evidence tools and mechanisms.
- Where applicable, the law shall establish in which circumstances electronic print-outs ("hardcopies) of electronic documents shall be deemed as meeting the requirements of the best evidence rule.
- The law shall establish that the admissibility of e-evidence shall be guided by the principles of functional equivalence, precaution, and accreditation.
- The law shall establish that computer forensics be employed in judicial discovery relating to e-evidence.
- The law shall regulate the circumstances which allow that the presumption of integrity of an electronic records system be established by means of an affidavit given to the best of the deponents knowledge and belief, and the possibility that said deponents be cross-examined.
- The law shall establish sanctions to any person who in an affidavit or certificate tendered makes a statement which that person knows to be false or does not believe to be true.
- The law shall establish criteria harmonizing sanctions against a person who has made untrue statements in an affidavit or certificate relating to the integrity of an electronic records system.
- The law/legal mandate shall provide for the establishment of appropriate search and seizure procedures, which will ensure the integrity of the evidence collected.

…/…

Section I

- The law/legal mandate shall provide for the establishment of procedures for the certification and production of data collected and also of the digital environment at the time of the collection of the data.
- The law shall establish recognition of private agreements on admissibility of electronic records (and may set forth that extension to criminal proceedings if subject to constraints).
- The law shall establish that parties are at liberty to agree to use a particular method of electronic signature, unless otherwise provided by law.
- The law shall establish that 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.
- The law shall establish that the Certificate Service Provider maintains available for a certain amount of time the tracking records of security procedures that it followed.
- The law shall establish that the certification authority is empowered and required to also certify the time of electronic records ("time-stamping").

4. CARICOM/CARIFORUM COUNTRIES SHALL PROVIDE ADEQUATE PROTECTION TO E-EVIDENCE

- There shall be a definition of "imaging" for the purposes of protecting e-evidence.
- The law/legal mandate shall establish that individuals be protected against prejudice regarding administrative or judicial admissibility of e-evidence.
- The law/legal mandate shall provide for recognition of the use of certified electronic time-stamping.
- The law/legal mandate shall provide for recognition of procedural standards in consideration of evidence reliability of data maintained in a specific electronic records system.
- The law/legal mandate shall also determine, possibly via Regulations, the boundaries of legal and illegal use of technologies such as cryptography, steganography, and remailing, relating to e-evidence.
- The law/legal mandate shall provide for recognition of images as e-evidence, and provide guidelines dissociating electronic images from "imaging".
- There shall be public policy to encourage the use of certification of attributes, in certificates of digital signature, to enhance the capability of identifying its holder and establish electronic evidence.
- The law/legal mandate shall encourage the use secure techniques (for instance, secure transmission via IP) when using teleconferencing with, to be applied in public service (for instance, in certain hearings to be carried out in judicial proceedings).
- The law/legal mandate shall encourage and recognize the proper use of cameras as a way to establish e-evidence.
- The law/legal mandate shall encourage and recognize the facilities which can be apportioned by telecommunications devices for establishing e-evidence.

Section I

5. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH THE FRAMEWORK OF E-EVIDENCE IN CONJUNCTION WITH PUBLIC POLICIES ON RELATED MATTERS

- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on national security.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on cybercrime.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on interception of communication.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on expedited preservation.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on production order.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on search and seizure.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on real-time collection.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on digital signature.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on privacy and on data protection.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on information security.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on intellectual property.
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on freedom of information.
- The law/legal mandate shall regulate e-evidence in a way consistent with treaties on the mutual recognition of official public documents (in conformity with The Hague Convention).
- The law/legal mandate shall regulate e-evidence in a way consistent with public policy on social digital inclusion.

Section II:
Model Legislative Text – Electronic Evidence

Following, is the Model Legislative Text that a country may wish to consider when developing national legislation relating to Electronic Evidence in e-Commerce. This model text is based on the Model Policy Guidelines outlined previously.

Arrangement of Sections

PART I – PRELIMINARY

Short Title 1. This Act may be cited as the Electronic Evidence Act, and shall come into force and effect on [xxx/ following publication in the [name of the publication].

Definitions 2. (1) Accredited certificate means a certificate issued by an accredited certification service provider.

(2) Addressee, in relation to an electronic record, means a person who is intended by the originator of such electronic record to receive it, and does not include a person acting as an intermediary with respect to that electronic record.

(3) Advanced electronic signature means an electronic signature provided by an accredited certification service provider.

(4) Authentication products or services means products or services designed to identify the holder of an electronic signature to other persons.

(5) Certificate means an electronic attestation which links signature – verification data to a person and confirms the identity of that person, or links time – verification data to an electronic record or to an electronic communication and confirm the date and time of which.

(6) Computer means any digital information system integrated by equipment and programs intended for creation, recording, storage, processing and/or transmission of data, including any computer, computer devices, or other electronic information or communication devices, intended to perform such functions.

(7) Content data means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form. Content data includes any data that conveys the meaning or substance of a communication as well as data processed, stored, or transmitted by computer programs.

(8) Cryptography service means any service which is provided to a sender or recipient of an electronic communication or to anyone storing an electronic communication, and is designed to facilitate the use of cryptographic techniques for the purpose of ensuring –

(a) that the data or electronic communication 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 electronic communication is capable of being ascertained;

(c) the integrity of the data or electronic communication; or

(d) that the source of the data or electronic communication can be correctly ascertained.

(9) Data (or computer data, or electronic data) means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable to cause an information system to perform a function.

(10) Digital signature means an electronic signature based on asymmetric cryptography including associated public and private keys.

(11) Electronic includes 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 means.

(12) Electronic agent means a program, computer, or other electronic or automated means, configured and enabled by a person, that is used to initiate or respond to an electronic record or event in whole or in part, without review by an individual.

(13) 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.

(14) Electronic communication means any transfer of records by means of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce , but does not include –

(a) any wire or oral communication;

(b) any communication made through a tone-only paging device;

(c) any communication from a tracking device.

(15) Electronic record means a set of data that is created, generated, recorded, stored, processed, sent, communicated, and/or received, on any physical medium by a computer or other similar device, and that can be read or perceived by a person by means of a computer system or other similar device, including a display, print-out or other output of those data.

(16) Electronic signature means any signature based on an electronic process, including digital signature, biometrical signature, and others.

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

(18) Law means the common law, legislation, and subordinate legislation.

(19) Legal proceeding means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

(20) Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

(21) Originator, in relation to an electronic record, means a person who –

(a) sends an electronic record;

(b) instructs another to send an electronic record on his behalf; or

(c) has an electronic record sent by his electronic agent but does not include any person acting as an agent or intermediary with respect to the sending of that electronic record.

(22) Public body includes:

(a) ministry or department of government;

(b) wholly or partially owned state companies or enterprises;

(c) bodies exercising statutory authority, of legislative, executive or judicial nature;

(d) sub-national or local public authorities, including municipalities.

(23) Record means recorded information collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide evidence or proof of that activity or transaction, inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form.

(24) 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.

(25) 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 or digital methods.

(26) Signature creation data means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

(27) Subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established:

(a) the type of communication service used, the technical provisions taken thereto, and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; and/or

(c) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement.

(28) Traffic data means computer data that:

(a) relates to a communication by means of a computer system; and

(b) is generated by a computer system that is part of the chain of communication ; and

(c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.

Section II

PART II – ADMISSIBILITY

Amendment to Authentication and Best Evidence Rules

3. This Act does not modify any common law or statutory provision relating to the admissibility of records, except those relating to authentication and best evidence.

Common Law and Statutory Rules

4. In applying any common law or statutory provision relating to the admissibility of records, the Court may have regard to the principles guiding the admissibility of electronic records as prescribed by this Act.

General Admissibility of Electronic Evidence

5. 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.

Application of the 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 computer in or by which the data was recorded or stored.

(2) In the absence of evidence to the contrary, the integrity of the computer 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.

Integrity of Information, and Specific Admissibility Rules

7. (1) A statement contained in an electronic record produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein unless the integrity of the computer is presumed under subsection 2.

(2) In the absence of evidence to the contrary, the integrity of the computer in which an electronic record is recorded or stored is presumed in any legal proceeding if the transaction record:

(a) has remained complete and unaltered, apart from:

(i) the addition of any endorsement; or

(ii) any immaterial change;

which arises in the normal course of communication, storage or display;

(b) has been electronically certified or has been electronically signed, by a method provided by accredited certification entities;

(c) which integrity and content has been notarized;

(d) has been recorded in a non-rewritable storage device, or any other electronic means that does not allow the alteration of the electronic records;

(e) has been examined and its integrity confirmed by an expert appointed by the court; or

(f) relating to which:

(i) 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.

(ii) 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) 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.

(3) Where a statement contained in an electronic record produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in subsection (2) are satisfied in relation to that electronic record.

Print-outs 8. In any legal proceeding, where an electronic recording 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.

Burden to Prove the Authenticity of Electronic Evidence 9. 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. In the event there is special legislation protecting more vulnerable persons, including consumers and children, and establishing allocation of burden of proof more beneficial to those persons, such legislation shall have precedence over this section.

Standards 10. For the purpose of determining under any other 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 used, recorded or preserved the electronic record and the nature and purpose of the electronic record. Public authorities in charge of development or approval of relevant technical standards or security procedures shall issue guidelines providing orientation on the applicable criteria to be followed for compliance with this section.

Affidavits 11. Where it is intended to adduce an electronic record as evidence, it is permissible to have that record adduced in the form of an affidavit.

Agreement on Admissibility of Evidence

12. (1) Unless otherwise provided in any 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 legally assisted or represented.

Electronic Signature

13. (1) An electronic signature is not without legal force and effect merely on the ground that is in electronic form.

(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.

Electronic Signature Requirements

14. (1) Where the 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 law provides consequences for the absence of a signature.

(3) Parties may agree to use a particular method of electronic signature, unless otherwise provided by law.

(4) 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 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.

(5) Subsection (4) 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.

(6) 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

(7) The Court shall have regard to any law that provides for the veracity of the authorship and integrity of digitally signed electronic records.

Alternative Techniques and Procedures for Production of Electronic Evidence

15. In addition to the means of proof referred to in the preceding sections in this Act, electronic evidence may be produced with regard to certain electronic record by means of alternative techniques and procedures, such as attestation by notaries public or justices of the peace or by other such authorities, recording on non-rewritable medium, and computer forensics in the course of judicial discovery.

PART III – GENERAL PROVISIONS

Admissibility of Electronic Records from Other Countries

16. Where electronic evidence originates from another jurisdiction, its admissibility is not impaired if the integrity of the computer associated with the relevant electronic evidence is proven or presumed in accordance with standards comparable to those provided for in sections 6 (2) (a), and 7 (2) of this Act.

Recognition of Foreign Electronic Documents and Signatures

17. (1) In determining whether or not, 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, provided the electronic record is located in domestic jurisdiction.

(2) Where the electronic record is located in a foreign jurisdiction, subsection (1) above does not apply unless –

(a) the party who adduces evidence of the contents of the electronic record has, not less than 14 days before the day on which the evidence is adduced, served on each other party a copy of the electronic record proposed to be tendered;

(b) the court directs that it is to apply; or

(c) there is international treaty in effect establishing recognition of electronic record s or of electronic signatures located in the foreign jurisdiction.

Interpretation in Accordance with Internationally Accepted Principles

18. The provisions of this Act shall be interpreted and enforced in light of the internationally accepted principles of technological neutrality and of functional equivalence.

Regulations

19. The Minister may make regulations for giving effect to the purposes of this Act and for prescribing anything required or authorised by this Act to be prescribed. In so doing the Minister may consider international best practices and standards.

Section III:
Explanatory Notes to Model Legislative Text on Electronic Evidence

INTRODUCTION

1. This legislative text develops a legal framework for admissibility of electronic records. The main objectives of this legislative text (Act) are to establish general admissibility of electronic evidence, amend authentication and best evidence legal rules, set forth the criteria which lead to presumption on integrity of computers and of electronic records, address relevant burden of proof, regulate admissibility of electronic signatures, determine interpretation based on internationally accepted principles, and contemplate recognition of electronic records originated or located in other countries.

2. These notes are aimed to explain the contents of this Act, and shall be read in conjunction with it. They explain the importance of key provisions of this Act and, where applicable, call attention to particular discussions held by the working group, highlighting different options of regulation discussed therein. They are not, and are not meant to be, a detailed description of this Act. So, where a Section or part of a Section does not seem to require any comprehensive clarification, comment or reference, or when there was no discussion concerning some particular provision, no detailed explanation is given.

3. This Act consists of three parts**:**

   - **Part I** provides definitions;
   - **Part II** amends authentication and best evidence legal rules, establishes the principle of non-discrimination against electronic records, regulates application of the Best Evidence Rule, defines criteria for presumption on integrity of computers and of electronic records, allocates burden of proof, determines issuance of guidance on compliance with technical standards and with security procedures, acknowledges agreement on admissibility of electronic evidence in judicial proceedings, recognizes electronic signatures as evidence, and addresses alternative technique and procedures for production of electronic evidence;
   - **Part III** establishes general provisions contemplating admissibility of electronic records from other countries, recognition of foreign electronic documents and signatures, interpretation in accordance with internationally accepted principles, and possible regulations aligned with international best practices and standards.

Section III

COMMENTARY ON SECTIONS

PART I – PRELIMINARY

4. Part I provides preliminary provisions such as short title and commencement clause in **Section 1**, and definitions in **Section 2**.

5. Part I has motivated a discussion within the working group with regard to drafting style in different jurisdictions. It was discussed whether it should include a Section outlining the objectives of this Act, and consensus reached was that such question should be left to the discretion of beneficiary state.

Section 2. Definitions

6. The definition of **Computer** provided by subsection (6) leaves room for encompassing any electronic device which may perform functions typical of computers.

7. There was a debate within the working group on whether there should be explicit reference to telecommunications equipment such as smart cell phones. It was agreed that the rapid pace of technological progress, together with the principle of technological neutrality, make it advisable to maintain broad wording mentioning "electronic information or communication devices", complementing the references to "computer" and to "computer devices".

8. **Content data** (together with location data and traffic data, which are defined respectively in subsections 20 and 28) are data which generation, communication, processing and storage are natural targets for production of electronic evidence, as they consubstantiate underlying communications and transactions.

9. The definition of content data has been worded in such a way ("essence, substance, information, meaning, purpose, intent, or intelligence") to comprise every kind of contents of an electronic record.

10. Such definition refers both to processed and to unprocessed forms of content data. The purpose here was to encompass not only "raw" contents aimed to be transformed in the course of data processing, but also the different data generated as output of such processing activity.

11. The definition at hand has also referred to "metadata", which is a second layer of data, containing "data about data" (such as the language used to write some contents, the time of its generation, where to find more about that contents, and so on). As the use of metadata and of metatags becomes increasingly popular (given, especially, the common usage of internet search engines driven by such metadata and metatags), metadata may provide important elements for production of electronic evidence regarding content data.

12. **Data** is defined in subsection (9) as representing facts, information, or concepts in a form suitable for processing in an information system.

13. Data was selected as defined expression in lieu of "information", which is an expression present in some countries' national legislation dealing with general evidence, not necessarily with electronic evidence. As the scope of this Act refers solely to electronic evidence, the intent here was to mean only the facts, information, and concepts which have been represented in electronic, binary digits form.

14. The working group has debated over the convenience or not of including the expression "state" in such definition, which would purport to emphasize that data may not only be logically conceived as sequences of "0" and "1" digits (which represent letters or numerals) but also mean the tangible change of electromagnetic or optical status in a computer which the information system "reads" as respectively corresponding to the binary digits. Although the expression "state" may help laymen

(including magistrates) take also into account the tangible aspect of data and so contribute to qualify data, legally, as "thing" (for establishing that it may be subject to possession or to misappropriation, among other purposes), the last portion of that definition, which mentions "including a program suitable to cause an information system to perform a function" may indirectly achieve, to some extent, the goal of also meaning the tangible character (as the performance of a function in an information system is expected to produce some tangible change). Therefore, preference for either level of emphasis on the tangible aspect of data was left to the discretion of beneficiary state.

15. Finally, such definition makes clear that data is a synonym of "computer data" and of "electronic data", which expressions are present in related legislation at countries' and international levels. Hence, correspondence between the former and the latter is guaranteed, for the sake of consistency, especially with regard to legislation from other countries, where the diversity of terminology employed is greater, enhancing the need of building bridges to facilitate common interpretation and enforcement.

16. **Digital signature** has been defined in subsection (10) as a particular type of electronic signature. In conjunction with definition of other expressions (such as **Accredited certificate, Advanced electronic signature, Authentication products and services, Certificate, Cryptography service, Electronic signature, Signature,** and **Signature creation data**) featured in other subsections of Section 2, it provides coherent meaning to a key system of production of electronic evidence – the system of authentication, certification, and accreditation of digital signatures – , capable of identifying authorship, origin, time, and other elements.

17. The definitions adopted for such set of expressions have taken into account that the beneficiary state may or may not have implemented determined technology or organization to build a system of certified electronic signatures, locally established or hired from abroad. For such reason, those definitions have concentrated on basic aspects, leaving for further regulation any possible more specific options (such as the different structure of roles and powers, the allocation of regional or national resources, and so on).

18. By taking such approach, the definition on digital signatures facilitates integration with other provisions of this Act, such as the ones relating to conformity with the Best Evidence Rule or to alternative means of production of electronic evidence, since the generic wording adopted provides flexibility to accommodate different manners of using digital signatures to evidence the integrity and reliability of a computer or of an electronic record, or to mirror or incorporate alternative forms of electronic evidence.

19. The automated electronic response used as interface for the interaction of human beings with computers characterizes the **Electronic agent** as defined in subsection (12). Such definition is one of the elements which integrate the concepts of originator and of addressee of an electronic communication, and may determine whether effective sending or receipt has taken place, and how and where it shall be evidenced.

20. Reliability of communications supported by electronic means is fundamental for the purpose of production of relevant electronic evidence. The concept of **Electronic authentication**, defined in subsection (13), helps determine the procedures which may be used to verify whether any given communication has been altered during transmission, and to ascertain who was its originator.

21. The definition of **Electronic communication**, contained in subsection (14), is important as it focuses on the transfer of records, including the respective sending and receipt, while the definition of "computer" or of "information system" are limited to focus on the internal activities performed by the computer or by the information system.

22. The working group has debated over the convenience or not of including reference to "any wire or oral communication". Some concern was voiced to the effect that such expressions might overlap with expressions existing in telecommunications laws of certain countries, especially with regard to telephony, paging, and tracking devices. The group has decided that it shall be left to the discretion of beneficiary state whether to maintain such wording or not.

23. Subsection (4) defines **Electronic record** as a set of data that can be read or perceived by a person by means of use of a computer system or other similar device.

24. While data is represented in binary form and purports to be "read" by a computer or "translated" by a computer program, electronic record is the appearance or output of an information system which can be perceived by a human being.

25. The distinction between those complementing expressions – "data", and "electronic record" – is necessary for the task of legislating on electronic evidence, since the proof on some facts, information, or concepts may rely on the perception by a person (or on the capability of being perceived by him/her) and not only on the possibility of technical discovery.

26. The definition of "electronic record" is also of interest for determining the meaning of "electronic information device" (which has been referred to in some provisions of this Act within the wording "electronic information or communication devices"), as it is clearly intended to mean a device used by human beings to access/perceive electronic records.

27. In addition, the definition of "electronic record" has incorporated the expression "on any physical medium", which is expected to contribute to expand the scope of media associated with electronic records, extending it beyond traditional media, to comprise, for instance, biometrical media (such as fingerprints, or the iris), which have been increasingly applied in the context of electronic evidence.

28. Similarly, the reference to print-outs clarifies that electronic records are not necessarily to be perceived in a computer system, and may rather be perceived as an element external to it.

29. Equally important for the understanding of the phenomena surrounding electronic evidence is the definition of **Information system**, contained in subsection (17). While the definition of "computer" means a single electronic equipment, the definition of "information system" purports to comprise groups of inter-connected devices, typical of electronic networks.

30. Such broad definition may include networks at various levels, including the Internet, which is technically considered a "network of networks". Given the magnitude of the Internet as scenery for production and gathering of electronic evidence, a specific reference was made to it. The concept of group of inter-connected devices is comprehensive enough to capture any equipment linked to the Internet.

31. The working group has debated on whether this Act should use the expression "computer system", or the expression "information system". The fact that "information system" (and "information-processing system) has been the one used in most countries' legislation has weighed in favour of it. Although there are some technical differences of meaning between "information system" and "computer system", they were considered not essential in the context of electronic evidence, therefore the option adopted was to use "information system", while adding "computer system" and "data processing system" as equivalent expressions. The level of technical accuracy wished for addressing such concepts in the context of this Act was left to the discretion of beneficiary state.

32. The definition of **Legal proceeding**, contained in subsection (19), includes not only civil proceedings but also criminal and administrative ones. While electronic evidence tends to be well assimilated in civil proceedings, it is often challenged in criminal proceedings, where it is invoked that its "virtual" nature does not constitute enough evidence to support a criminal conviction. Similarly, the "intangible" aspect commonly associated with electronic evidence may be disregarded in the

administrative sphere, leaving for judicial proceedings the task of evaluating such evidence. Therefore, it is important to make it clear that properly produced electronic evidence shall be valid for any proceeding, irrespective of being it civil or criminal, judicial or administrative.

33. The place where equipment is located is an important element for production of electronic evidence as it may imply different findings and consequences such as attribution of jurisdiction and of governing laws, determination of the level of security required and relevant liability, indication on the originator of documents or of communications, evidence on their effective sending or receipt, and so on. The definition of **Location data**, in subsection (20), recognizes the importance of the geographic position of equipment for production of evidence in the context of electronic communications networks.

34. Such definition has selected "terminal equipment" as parameter for determination of the geographic position, as this expression is flexible enough to encompass not only computers but also any device which can be used in the context of an electronic communications service.

35. Equally worth of note, such definition has limited the scope of determination of geographic position to "publicly available" electronic communications services, which may contribute to balance security reasons for the need to identify geographic position and privacy requirements, where applicable.

36. The concept of **Originator**, defined in subsection (21), is comprehensive enough to include not only the person who actually sends an electronic communication but also the person who instructs another to send on behalf of the former, as well as the person who uses an electronic agent for sending.

37. The comprehensiveness of such concept is increasingly important as the volume of electronic communications "sent" through third parties (as in "electronic call centers") or through electronic agents (as in the so-called "web-wrapping agreements") grows at a rapid pace.

38. The working group has decided to include a remark to the effect of clarifying that "electronic agent" does not include persons. Such remark is consistent with the definition of "electronic agent" in subsection (12).

39. **Public body** is defined in subsection (22) as including any ministry or department, state-owned companies or enterprises, bodies exercising statutory authority, and sub-national or local public authorities.

40. Such comprehensive definition is in line with the definition of **Law** which appears in subsection (18) and includes common law, legislation, and subordinate legislation, as well as with the observation in topic 17 above which mentions the possibility of further regulation establishing a system of authentication and/or certification of digital signatures. The issue here is that electronic evidence presents a broad array of implications for state bodies and for every citizen, so the diversity of legislation which may regulate it, as well as the number of authorities or of state-owned companies or enterprises which may use it, or which may regulate it, is quite large, so the relevant definition shall be comprehensive enough.

41. Although this Act does not contain an expressive number of provisions which make use of such definition (or make indirect use of it, as in Section 10, which refer to "public authorities"), it pre-establishes the large scope of public bodies expected to issue or to be beneficiary of further regulation (as in the quoted example of creation of a system of authentication and/or certification of digital signatures), ensuring appropriate grounds for future subordinate legislation.

42. The definition of **Security procedure** contained in subsection (24) goes beyond the contents of the definitions of "authentication products or services" and of "electronic authentication", respectively addressed in subsections (4) and (13), as the presumption of integrity of a computer relies in the adoption of security procedures independently of any possible tests based on electronic authentication, as well as the technical standards relating to information security are basically of procedural nature and not necessarily require the use of any authentication products or services. Therefore, the definition of "security procedure" is an important additional ingredient to legitimate the production of electronic evidence.

43. The wording of such definition has incorporated not only security procedures subject to technical standards but also the ones established by law, by agreement, or by known common practice, as it is important to recognize the free will of interested parties to negotiate the level of security procedures wished, as well as the existence of best practices in the field at national and/or international levels.

44. **Subscriber information** is a concept defined in subsection (27) with the purpose of comprising subscriber's enrolment data and any data relating to documents or to communications involving the subscriber of an electronic communication service.

45. Enrolment data may be an important element for production of electronic evidence, especially where anonymous communication is concerned, which enhances the need to know details such as name, identity documents, and address of the subscriber.

46. Similarly as to what happens with the definition of **Public bodies**, "subscriber information" is a concept of interest for further regulation on electronic evidence (and/or of related matters such as liability of Internet services providers for keeping and informing subscriber data), and the importance of pre-establishing it in this Act consists on guaranteeing uniform meaning for its later use.

47. Subsection (28) addresses **Traffic data** aiming to comprise data of interest to production of electronic evidence regarding flow of electronic communications. Details such as origin, route, destination, date, time, size, and duration are very important for determining authorship, place, and time of certain actions, especially where electronic communication flows split by "packages" which may follow different paths up until reaching their intended destination, as in the Internet.

PART II – ADMISSIBILITY

Section 3: Amendment to Authentication and Best Evidence Rules

48. The main purpose of this Section is to determine the integration of this Act with common law and with statutory provisions which regulate admissibility of records, clarifying that the only legal rules amended by this Act are those which deal with authentication and with the Best Evidence Rule.

49. By specifying which laws have been amended, such Section automatically implies that the laws not amended by this Act shall also apply to the matters regulated by it. The matters covered by this Act shall thus be viewed as a specific chapter within the field of application of more general principles of admissibility of evidence.

Section 4: Common Law and Statutory Rules

50. The purpose of this Section is to establish that in the application of common law or of statutory rules which address admissibility of records, Courts shall take into account the provisions of this Act where electronic records are to be considered. It is important that Courts recognize the specificity of the matter and of the provisions contemplated by this Act, so this Section purports to call attention of magistrates to the need of enforcing this Act.

Section III

Section 5: General Admissibility of Electronic Evidence

51. This Section establishes the principle of non-discrimination against electronic records. Any record may or may not be reliable as evidence, irrespective of being electronic or not. Hence, there is no reason for discriminating *a priori* against electronic records. It can even be said that certain electronic records (such as in the case of certified digital signatures) may be more trustworthy than non-electronic records.

52. The importance of this Section is that it sets forth the admissibility of electronic records as a general rule, subject to the requirements listed in the subsequent Sections.

Section 6: Application of the Best Evidence Rule

53. Being the Best Evidence Rule a traditional principle of law in the Common Law system, it is important that legislation on electronic evidence be compatible with such principle.

54. In order to harmonize the application of such principle with the characteristics of computers, this Section has established that the Best Evidence Rule is considered satisfied where the integrity of a computer in or by which certain data was recorded or stored can be evidenced.

55. As the Best Evidence Rule requires presentation of the originals of a given document but one can hardly determine whether some electronic data is an original or a copy, the proof of integrity of a computer is an adaptation, *mutatis mutandis*, of the traditional intent of the Best Evidence Rule.

56. Such adaptation has legal, technical, and economic reasons. Legally, the philosophy behind the Best Evidence Rule is to ensure that the best possible evidence (normally, the originals of some document) is presented. From the technical and economic standpoints, it is not plausible to implement the technologies and procedures (such as certified digital signature) which may be equivalent to an original in all electronic records of an information system. Therefore, the conjunction of legal, technical and economic reasons indicate that the proven integrity of a computer is the best possible evidence in normal circumstances.

57. The situations which authorize presumption on integrity of a computer are listed in subsection (2), and basically allow it (i) where evidence is adduced supporting the finding that the computer was operating properly, (ii) where the electronic record was recorded or stored by a party who has opposite interest to the party who seeks to introduce it in a proceedings, or (iii) where the electronic record was recorded or stored by whom is not a party to a proceedings or whom did not record or store the electronic record under control of a party seeking to introduce it. In short, such presumption applies where there is evidence on the proper operation of a computer or where there is no conflicting or suspicious interest of the party who seeks to introduce the electronic record in a proceedings.

Section 7: Integrity of Information, and Specific Admissibility Rules

58. The presumption on integrity of computers contemplated in general terms in Section 6 is also addressed by the provision contained in Section 7, which brings in its subsection (2) a list of situations where the integrity of an electronic record induces the presumption of the integrity of the computer, in any legal proceedings, independently of whether the electronic record constitutes hearsay or not (as contemplated in subsections (1) and (3), respectively).

59. Such list starts by making reference to transaction records (i.e., electronic records) which have remained complete and unaltered apart from immaterial changes arisen in the normal course of communication, storage or display. Such wording is important given that computers and electronic records can hardly be “frozen” and kept immune from any sort of change, and that it limits the scope of change which may really compromise the reliability of an electronic record.

60. The second situation contemplated refers to records electronically certified or electronically signed by a method provided by accredited certification entities. The convenience of establishing accredited certification authorities or entities can be clearly noticed here as such accreditation ensures a formal presumption by itself and thus contribute to induce the presumption on material integrity of the electronic record.

61. The list proceeds by mentioning the alternative of notarized integrity and content, which is another option available to interested parties and may be of interest as public notaries can attribute faith to the integrity and content they may witness.

62. The fourth hypothesis consists on the recording in non-rewritable media, which, by definition, does not allow any change once an electronic record is stored at the first time. This may be a practical and convenient option for the interested parties who wish an easily available and less expensive alternative.

63. The fifth situation is that of technical discovery in Court proceedings, where the expert appointed by the judge can confirm the integrity of the electronic record.

64. The diversity of situations which authorize presumption on integrity of an electronic record and extends to presumption on integrity of a computer is important as every interested party shall have access to a number of practical means of production of electronic evidence.

Section 8: Print-outs

65. Although a print-out is not by itself electronic, it is generated by electronic means. Therefore, if the interested parties have consistently accepted it as a true representation of the corresponding electronic record, the reliability which can be inferred from such conduct of the parties authorizes the finding that it satisfies the Best Evidence Rule. This is what Section 8 has provided for, and it is important as most people use to print electronic records concerned with electronic evidence.

Section 9: Burden to Prove the Authenticity of Electronic Evidence

66. As a general rule, the person seeking to introduce an electronic record as evidence has the burden to prove relevant authenticity, in any legal proceeding.

67. However, more vulnerable persons such as consumers and children may be benefited by statutory provisions which invert the burden of proof. In such event, those statutory provisions shall prevail over the general rule established in Section 9.

68. Such remark is important because more vulnerable persons are usually not technically and/or economically able to produce evidence based on electronic records, but nevertheless their access to Justice and to the opportunity of counting on proper defence shall be promoted and ensured.

Section 10: Standards

69. Common practices and usages are an important indication on what shall be expected as pattern of conduct for the recording or preservation of electronic records. Therefore, evidence may be presented on existing standards, procedures, usages or practices which reflect such pattern and provide guidance on what is expected regarding admissibility of electronic records.

70. Section 10 contemplates recognition of such guidance and links it to the type of business or endeavour it refers to as well as to the nature and purpose of the electronic record. Such linking is important as the standards applicable to a certain market may present objectives different than the ones applicable to another market (as it is the case where information security is involved).

71. This Section ends by convoking public authorities in charge of issuing technical standards or of establishing security procedures to provide appropriate orientation on compliance with this Section. This is important as the competent authorities can and shall provide general orientation as well as orientation tailored to individual markets or circumstances, where applicable.

Section 11: Affidavits

72. Section 11 establishes that electronic evidence may be presented in the form of affidavits. This is one more alternative of production of electronic evidence which is available to interested parties.

73. The working group has debated over convenience of including other provisions in this Section such as a statement that every deponent has the duty to give affidavit to the best of his knowledge or belief, and that he is subject to sanctions imposed by Courts in the event his affidavit is found to be untrue, besides a provision on cross-examination of affidavits.

74. Given the fact that electronic records are of a volatile nature, dependence on affidavits may be a point of concern, and therefore might be balanced with some emphasis on liability of the deponent. However, regulating on this may overlap with existing procedural norms. Hence, the working group has decided that adoption of the referenced approach shall be left to the discretion of beneficiary state.

Section 12: Agreement on Admissibility of Evidence

75. As a general rule, unless no other law provides otherwise, the parties to a legal proceedings may agree on the admissibility of any given electronic record, subject to the discretion of the Court.

76. This provision shall not apply to criminal proceedings where the accused persons were not legally assisted or represented at the time such agreement was reached.

77. Section 12 is important as it favours private agreement, avoiding controversies, which might otherwise determine unnecessary Court proceedings costs and delays.

Section 13: Electronic Signature

78. Similarly to what has been provided for by Section 5 with regard to electronic records, Section 13 establishes in its subsection (1) that electronic signatures shall not be discriminated solely for the reason that they are in electronic form.

79. Subsection (2) expresses the possibility that electronic signatures are proven in any manner. Given the rapid pace of technological advances in the field of electronic signatures as well as the importance of complying with the principle of technological neutrality, it seems unlikely that the existing different manners of proof of electronic signatures could be properly circumscribed.

80. An illustrative example of how diverse can be the manners of proof of electronic signatures is given in the same subsection, by referring to proof of existence of a procedure whereby a person must execute a symbol for the purpose of verifying that an electronic record is that of such person (what is quite common in world wide web sites as a condition to allow Internet users to enter into specific areas of such web sites).

Section 14: Electronic Signature Requirements

81. Subsection (1) of Section 14 establishes that electronic signatures meet law requirements of signature of a person where they are as reliable and appropriate. This provision is important as electronic signatures can effectively be reliable and appropriate and in some cases even more than non-electronic signatures.

82. Subsection (3) determines that parties are free to agree on use of any particular method of electronic signature unless otherwise provided by law. This provision is important as it is consistent with general principles of freedom to establish evidence, while it provides a remark which may be applicable, for instance, where the use of electronic signatures based on cryptography may collide with individual privacy or national security laws.

83. Parties to an agreement may not specify the type of electronic signature to be used by them. Such situation is quite common in practice, so subsection (4) addresses it providing a list of criteria for meeting contractual requirements on electronic signing data messages. Referenced criteria include the linking between the signatory and the signature creation data (which shall be under control of the signatory), and the possibility of detecting any alteration to the electronic signature at the time of signing or after it.

Section 15: Alternative Techniques and Procedures for Production of Electronic Evidence

84. Section 15 refers to alternative techniques and procedures for production of electronic evidence with regard to certain electronic records, quoting (i) attestation by notaries public or justices of the peace or by other authorities, (ii) the recording of the electronic record on non-rewritable medium, and (iii) computer forensics in the course of judicial discovery.

85. The recognition of computer forensics, which is a field of knowledge specialized in electronic evidence, is very important, especially as it has been associated with judicial discovery, what makes it become even more reliable as the expert appointed by the judge is expected to be a neutral and qualified professional.

PART III – GENERAL PROVISIONS

Section 16: Admissibility of Electronic Records from Other Countries

86. Section 16 stipulates admissibility of electronic records originated from another jurisdiction, provided the integrity of the computer can be proven or presumed in accordance with the same standards which apply to proof of integrity of electronic records originated in the domestic jurisdiction (i.e., evidence that the computer was operating properly and that the integrity of the electronic record was preserved).

87. This provision is important for the secure flow of electronic communications with other countries, which is essential for the interests of beneficiary state to expand electronic communications and businesses with other countries.

88. Given the fact that each country has its own rules on electronic evidence, the definition of a minimum requirement, by solely requiring evidence on integrity of computers or of electronic records, may facilitate the task of establishing a common denominator.

Section 17: Recognition of Foreign Electronic Documents and Signatures

89. While Section 16 deals with electronic records originated from other countries, subsection (2) of Section 17 addresses electronic information located in other countries.

90. Such subsection lists situations which may determine equivalent treatment to be given to information located in a foreign jurisdiction as compared to information located in the domestic jurisdiction. Among those are Court determination in such sense and the existence of international treaty ensuring relevant recognition.

91. Such provision is important as it may reinforce secure flow of electronic communications and transactions between beneficiary state and other countries. As electronic records located abroad may be technically more difficult to access for purposes of ascertaining its integrity, this provision guarantees procedures and situation which may overcome such possible technical constraints.

Section 18: Interpretation in Accordance with Internationally Accepted Principles

92. Section 18 determines that this Act be interpreted and enforced in light of the principles of technological neutrality and of functional equivalence, which are internationally accepted principles.

93. Those principles have been adopted by virtually all countries which have regulated electronic evidence and relating aspects. The principle of technological neutrality favours social digital inclusion as it enhances the possibility of development or of use of technologies similar to each other, which fosters greater access and lower prices. The principle of functional equivalence sustains that no restrictions shall be imposed to the on-line environment which are not present in the off-line universe, which tends to stimulate migration of communications and of transactions to the former.

94. This provision is important as it determines that such principles apply to any provision of this Act, what shall drive its interpretation and enforcement towards the social and economic goals envisaged by such principles.

Section 19: Regulations

95. Section 19 empowers the Minister to make regulations for giving effect to the purposes of this Act and for prescribing anything required or authorised by it to be prescribed, and adds that the Minister may consider international best practices and standards.

96. The purpose of this Section is to recognize and call attention to the convenience of issuing further regulation in order to ensure proper implementation of this Act.

97. In this regard, the working group has debated over some matters which shall be addressed in international treaties or in domestic regulation.

98. Matters such as an accreditation system for electronic signatures (including authentication, certification, and accreditation of digital signatures, attributes, and time), integration with procedural laws (for instance, for ensuring that the performance of search and seizure, production order, real-time collection, videoconferencing of interrogatory, electronic judicial proceedings, expedited preservation of data, and interception of communication comply with this Act), and integration with related substantive laws (on data retention, liability of Internet services providers, and on cyber-crime, among others) have been found to deserve attention of domestic regulators.

99. Challenging trends such as cloud-computing, steganography, LiveCD, and others which may represent points of concern for production and recognition of electronic evidence have been considered as deserving special studies. The importance of carrying out such studies, as well as of issuing referenced regulation, is that enforcement of this Act may otherwise be weakened or obsolete.

100. Development of regional law, and harmonization with international treaties, has been deemed of interest to the beneficiary state in order to guarantee formal cooperation with other countries and periodical monitoring and alignment with then-current international best practices. The importance of such development and harmonization is that enforcement of this Act may otherwise be limited in scope or reduced to “informal” cooperation.

ANNEXES

Annex 1

Participants of the First Consultation Workshop for HIPCAR Project Working Group 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
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel

Annex 1

Country	Organization	Last Name	First Name
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 Consultants Participating in the Workshop

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

[7] Workshop Chairperson

Annex 2

Participants of the Second Consultation Workshop (Stage B) for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues Crane, St. Philip, Barbados, 23-26 August 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 and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Economic Affairs, Empowerment, Innovation, Trade	NICHOLLS	Anthony
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of the Civil Service	STRAUGHN	Haseley
Barbados	University of the West Indies	GITTENS	Curtis
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Government of Dominica	ADRIEN-ROBERTS	Wynante
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Tourism and Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Guyana	Office of the President	RAGHUBIR	Gita
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Jamaica	Ministry of National Security	BEAUMONT	Mitsy
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Department of Technology, National ICT Centre	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Lucia	Ministry of Communications, Works, Transport & Public Utilities	FELICIEN	Barrymore
Saint Vincent and the Grenadines	Ministry of Telecommunication, Science, Technology and Industry	ALEXANDER	Kelroy Andre

Annex 2

Country	Organization	Last Name	First Name
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Ministry of Trade and Industry	SAN A JONG	Imro
Suriname	Ministry of Transport, Communication and Tourism	STARKE	Cynthia
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	PELSWIJK	Wilgo
Suriname	Telecommunicatiebedrijf Suriname/Telesur	JEFFREY	Joan
Trinidad and Tobago	Ministry of National Security	GOMEZ	Marissa
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Ministry of the Attorney General, Attorney General's Chambers	EVERSLEY	Ida
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PERSAUD	Karina
Trinidad and Tobago	Telecommunications Services of Trinidad and Tobago Limited	BUNSEE	Frank

Regional/International Organizations' Participants

Organization	Last Name	First Name
Caribbean Centre for Development Administration (CARICAD)	GRIFFITH	Andre
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
ALMEIDA	Gilberto Martíns de
GERCKE	Marco
MORGAN[8]	J Paul
PRESCOD	Kwesi

[8] Workshop Chairperson.

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