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

Electronic Transactions: 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 Transactions:

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.

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, Mr. Kwesi Prescod and Ms. Karen Stephen-Dalton. 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. Gilberto 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 Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Cybersecurity Division (CYB) as well as from Mr Michael Tetelman. Support was provided by Mr Philip Cross, ITU Area Representative for the Caribbean. Some pre-formatting was done by Mr. Pau Puig Gabarró. The team at ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Page

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 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).

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

[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 funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). HIPCAR 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.

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.

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 Commerce (Transactions), 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 Transactions in the HIPCAR beneficiary countries and the identification of potential gaps in this regard, thus providing the basis for the development of the model policy framework and legislative text presented herein. By reflecting national, regional and international best practices and standards 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.

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

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, Mr. Kwesi Prescod and Ms. Karen Stephen-Dalton. The model legislative text on Electronic Transactions was developed in three phases initially by HIPCAR consultants: (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 documents were 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 Gilberto Martíns de Almeida addressing, *inter alia*, the points raised at the second workshop. 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 Transactions

In a world of economic globalization, domestic and international trade are increasingly wide-spread and intertwined. Their performance and integration are today being carried out mainly through electronic transactions that allow for the instantaneous flow of business to any market. The trust required for conducting business in such a way relies particularly on the existence of specific statutory laws establishing the conditions for relevant enforceability. Not having such legislation means not offering a safe legal environment for electronic commerce (e-commerce).

Internet banking, electronic broking of securities, clearing and custody of commercial or financial electronic records, mobile payments, electronic ordering of financial investments and closing of export-related bank electronic exchange contracts are just some examples of the myriad situations which are expected by local and by international communities to be supported by e-commerce laws.

This expectation has translated into approval of specific international conventions[4] and model laws[5] which aim to inspire the corresponding legal provisions in each country and avoid significant differences in regulation by individual countries. Consistency with such basic frameworks has turned into a pre-requisite for an appropriate legal platform for e-commerce.

The Model Policy Guidelines and Model Legislative Text contained in this document have been drafted in accordance with the frameworks referenced above so as to provide HIPCAR's beneficiary countries with drafting guidelines that are reasonably aligned with international best practices.[6]

Moreover, e-commerce[7] is today a key component in achieving economic growth by ensuring the timeliness and accuracy of contractual and financial transactions. This allows for – among other things – implementation of e-government services, improving the quality and reducing the cost of services, and increasing transparency and efficiency in the procurement and sale of goods and services.

---

4 Especially the *United Nations Convention on the Use of Electronic Communications in International Contracts, 2005,* which has been signed by a number of countries ranging from very large ones such as China and the Russian Federation to smaller ones such as Colombia, Honduras, Madagascar, Montenegro, Panama, Senegal, Sierra Leone, and Sri Lanka.

5 Including the *Commonwealth Model Law on Electronic Evidence*, the scope of which extends to cover certain aspects of electronic commerce.

6 The final model legislative text has also reflected the consensus reached among HIPCAR beneficiary countries based on their perceived common requirements. Subsequent drafting or review of individual countries' legislation may provide an opportunity for further adaptation of the model to local needs, for improving its consistency with international standards, or for contemplating reservations on certain of the matters that it covers.

7 E-commerce may be given different meanings and scope, including electronic formation of contracts, electronic communication of offline contract deals, electronic payments, and provision of government electronic services.

Introduction

In order for beneficiary countries to facilitate innovation and enhance their competitiveness by becoming active players in e-commerce, an environment to enable electronic transactions must be created that can assure equal opportunities while affording legal protection for consumers as well as business and industry operating in a global environment.

Recognising that traditional contract law has proven extremely adaptable and resilient to the changing demands of business, international organizations undertaking work in the definition of model frameworks for Electronic Transactions have endorsed a strategy of defining and establishing legal equivalences in this domain to key aspects of the contract formation process. In this way, the broader precedent of contract law remains unchanged and applicable.

Several international organizations have contributed to promoting the development of legislative frameworks for e-commerce, including:

- The *Commonwealth* – encompassing most of the HIPCAR beneficiary countries – has developed a *Model Law on Electronic Evidence*, helping to establish recognition of widely accepted standards that are particularly relevant to e-commerce.
- The *United Nations Commission on International Trade Law (UNCITRAL)* – established by the United Nations (UN) in 1966 to harmonize international trade law – is the core legal body that works to create accessible, predictable and unified commercial laws and has promoted model laws specifically regarding Electronic Transactions as well as the International Convention referred to above.
- The *Organisation for Economic Co-operation and Development (OECD)* has facilitated the creation of international instruments, decisions and recommendations that also provide guidance for individual countries operating in a globalized economy.
- The *European Commission's* Directives are geared to enabling harmonized legislative frameworks to support, among other things, cross-border trade in goods and services among its Member States. The *Directive on Electronic Commerce* and the *Directive on Electronic Signatures* provide the overarching legal framework in this area for this trade bloc.

The most important elements of e-commerce law relate to the fundamental components of commercial transactions: how to ensure that an online contract is as valid and enforceable as one carried out offline. The building blocks of e-commerce law therefore focus on both enforcing the validity of electronic contracts and ensuring that the parties can be held to their agreements. Once the contractual issues have been addressed, e-commerce law analysis shifts to a series of legal issues that may govern the transaction. These include jurisdiction (*i.e.*, which court or arbitral tribunal can adjudicate a case), consumer protection issues, taxation, privacy, domain name disputes, as well as the role and potential liability of intermediaries such as Internet service providers.

A key consideration in the determination of electronic-paper equivalence is the question of authenticity of electronic documents and the use of appropriate signing technologies to assure such authenticity. The administration of providers of such services is therefore essential in assuring commerce and consumers alike of the reliability of electronic commerce transactions. The challenge for policy-makers is to balance the imperative to establish trust with the reality of technology's dynamism, the availability of internal capacity and the global nature of the marketplace.

Any existing legal impediments that prevent the use of electronic communications to communicate legally-significant information must be removed, thereby creating a more secure legal environment for e-commerce. In establishing a legislative framework for electronic commerce, the legislation must be neutral in relation to technology and not restricted to specific technological solutions. It must also be flexible and adapted to be in harmony with developments in international rules and guidelines. Furthermore, the fundamental principles of law should remain uncompromised, and the legislation should contribute to establishing confidence in electronic commerce by providing for the protection and privacy of consumers.

Section I:
Model Policy Guidelines – Electronic Transactions

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Electronic Transactions.

1. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH NECESSARY COMMON INTERPRETATIONS FOR KEY TERMS ASSOCIATED WITH THE INFORMATION SOCIETY

- There shall be a definition for "electronic" which shall provide for technology neutrality in its application.
- There shall be an accompanying set of regulations that are subject to judicial construction and regular revision at the level of the State so as to determine the form and technology that allow for validity of a record or document.
- There shall be clear definition of who will be deemed the legitimate parties involved in a transaction conducted via electronic means, including the originator and addressee of a communication.
- There shall be clear definition of the persons who will be deemed as "intermediaries" in the facilitation of an electronically mediated transaction.
- There shall be a distinction between "intermediaries" and "telecommunication service providers" to consider the contexts where the terminologies denote either a sole entity or distinct entities.
- There shall be determination of the obligations of all legitimate parties involved in an electronic transaction, including the internet service provider and/or intermediary, the originator of a communication and the addressee of a communication.
- There shall be clear definitions for "information system" and/ or "computer" which is in accordance with other legal frameworks related to the information society.
- There shall be clear definitions related to the terms "record" and/ or "data message" so as to ensure conceptual distinction between the two terms.
- There shall be clear definition of the "electronic signature" which is:
  - technology neutral and distinct from an "advanced electronic signature" or "digital signature," which shall also be technology neutral.
  - clear on the distinction between an electronic signature as a tool of data authentication as opposed to identity identification
- There shall be clear definition of the term "certificate" or "qualified certificate" and the relevance of such a certificate in the context of signatory and advanced electronic signatures in the information society. There shall be clear definition of the "certificate service provider", its role and functions as opposed to that of the "certifying authority".

Section I

2. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH THE NECESSARY FRAMEWORK TO PROVIDE FOR ELECTRONIC DOCUMENTS AND TRANSACTIONS HAVING LEGAL EFFECT

- There shall be provision in law which explicitly states that the State is bound by the law/legal mandate establishing the Electronic Transactions framework.
- The law/legal mandate shall explicitly state that the use of electronic means in the execution of a contract or transaction is to be voluntary by both parties, and that the conditions regarding conditions of contract formation may be altered for a given transaction subject to the agreement of both parties.
- The law/legal mandate shall provide for the consent of a person to be inferred from prior actions. The principle of inference of consent shall be exempted in the instance of Public Authorities who shall be obliged to explicitly state consent.
- The law/legal mandate shall specify the types of transactions, or types of document for which the Electronic Transactions framework will have no effect. The types of transactions or documents which may be exempted must be characterized as being of particular value due to their singular existence. As such, these may include:
  - Instruments of inheritance, including Wills and Trusts.
  - Contracts for the sale or conveyance of real property.
  - Instruments effecting the grant of Power-of-Attorney.
- The law/legal mandate shall provide for the amendment of the list of exemptions by the Parliament.
- There shall be a set of regulations that shall consider the gradual inclusion of present exemptions subject to meeting specific law requirements as set by the relevant public authority within a jurisdiction.
- There shall be provision for Regulations with guidelines for all institutions that engage in electronic transactions to fulfil appropriate technical standards in encryption, authentication, back up, recovery and disposal of data.

3. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE THE STANDARDS TO WHICH ELECTRONIC DOCUMENTS MUST ADHERE TO BE CONSIDERED LEGALLY VALID

- 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 electronic documents will not be denied validity per se solely because the documents are electronic in nature.
- The law/legal mandate shall state that information shall not be denied legal effect solely because that information is referred to but not contained in an electronic document.
- The law/legal mandate shall provide for an electronic document to be deemed legally valid if it can assure its authenticity by remaining materially unchanged, and can be retained and stored by the receiving party.
- The law/legal mandate shall provide for a legally valid electronic document meeting any statutory requirement or rule of law for information being presented in writing.
- The law/legal mandate shall provide for a legally valid electronic document to be admissible with appropriate evidential weight.

- The law/legal mandate shall provide for an electronic document meeting any obligation of statute or rule of law requiring the presentation of information in its original form if the information was originally collected by electronic means, and there is reliable assurance that the information remains unchanged. The law/legal mandate shall provide for the standard of reliability to be assessed based on the purpose for which the information is required.
- The law/legal mandate shall provide that an electronic document including a valid electronic signature will deemed a valid electronic document and as effective as document containing a non-electronic signature.

4. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE DEFAULT CONSIDERATIONS TO BE APPLIED IN THE FORMATION OF CONTRACTS BY ELECTRONIC MEANS

- The law/legal mandate should be enabling in nature and refrain from being overly prescriptive in its provisions.
- The law/legal mandate should provide for the presumption that an electronic document or data message is sent by the originator once there is sufficient reason to believe that the document or message was sent by the originator or an individual or electronic agent acting on the originator's behalf.
- The law/legal mandate should provide for the presumption that an electronic document or message is received, in the general instances where there may or may not be an agreement between the parties of the sending of acknowledgement notices.
- The law/legal mandate should provide general guidance as to the conditions to be satisfied where either party may not apply the general presumption of attestation.
- The law/legal mandate should provide for the determination of when an electronic data message is deemed to have been sent as that time it is recorded to have left the information system or resource under the control of the originator.
- The law/legal mandate should provide for the determination of when an electronic data message is deemed to have been received as that time it is recorded to have entered an information system or resource under the control of the originator.
- The law/legal mandate should provide for the determination of the effective address of either party, the originator or addressee, in an electronic transaction.
- The law/legal mandate provides for the how errors in the preparation or transmission of an electronic document or data message is to be treated, with particular consideration for:
  - The general instance where the error is noted before any subsequent action has been taken by either party;
  - The general instance where the error is noted after subsequent action has been taken by either party, but before such action may be reasonably reversed by the action of the parties;
  - The general instance where the error is noted after subsequent action has been taken that cannot be readily reversed.

Section I

5. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH FRAMEWORKS FOR THE USE OF ELECTRONIC SIGNATURES, AND PROVIDE FOR THE PROPER ADMINISTRATION OF PROVIDERS OF SUCH SERVICES IN THEIR JURISDICTIONS

- The law/legal mandate should be technology neutral in nature.
- The law/legal mandate shall ensure that electronic signatures are related to the authentication of data or information within an electronic document or record.
- The law/legal mandate shall identify electronic signatures in such terms to provide broad applicability of technologies, while achieving the objective of:
  - Adequately identifying the signatory, and indicating the signatories approval of the information to which the signature relates; and
  - appropriate reliability for the purpose for which it was used.
- The law/legal mandate clarifies the obligation of the person relying on an electronic signature to verify reliability of the electronic signature.
- The law/legal mandate may specify types of "advanced" electronic signatures which are more sophisticated in nature, and require greater tests of applicability. The identification of such advanced electronic signatures should as much as possible refrain from the use of specific technologies or methodologies of digital signing.
- The law/legal mandate may specify greater recognition of authentication capacity of advanced electronic signatures. Where there is such recognition the law/ legal mandate may provide for the determination of specific legal requirements be met by advanced signatures exclusively.
- The law/legal mandate shall provide recognition of "certificates" which provide attribution of electronic signatures to particular signatories under specified conditions. The law/ shall provide for the greater validity of certificates qualified as being issued in accordance with industry standards and practices to enhance reliability associated with advanced electronic signatures.
- The law/legal mandate shall provide for the recognition of certificates issued by parties irrespective of where that certificate was issued, or where that party is located.
- The law/legal mandate shall provide for the establishment of persons within the jurisdiction who provide third party electronic signature generation services, as well as the generation, issuance and management of associated certificates (hereinafter referred to as "certificate service providers").
- The law/legal mandate shall limit the non-tariff barriers of entry to such service providers to that which is necessary to ensure oversight of appropriate general business practice.
- The law/legal mandate shall provide for the definition of appropriate operational requirements to ensure confidence of the public in the operation of certificate service providers established in the jurisdiction.
- The law/legal mandate shall ensure that the service provider issuing a certificate is liable for any damage caused by the reliance of that certificate where guidelines for appropriate use of the certificate is adhered to by the person relying on that certificate.
- The law/legal mandate may establish a designated agency responsible for the ongoing verification that service providers established in the jurisdiction operate in alignment with industry and business best practice.

6. CARICOM/CARIFORUM COUNTRIES SHALL PROVIDE MINIMUM REQUIREMENTS OF PERSONS TRADING THROUGH ELECTRONIC MEANS TO FACILITATE ADEQUATE CONSUMER PROTECTION IN AN ELECTRONIC ENVIRONMENT

- The law/legal mandate shall oblige persons who offer goods and services to trade ("vendors") through electronically mediated means to provide certain minimum information to the consumer, such information must include:
- The legal name, principle geographic address and forms of contact for the vendor,
  - Specific details of the items made available for sale, or the service being offered;
  - Terms, conditions and methods of payment;
  - The means by which queries can be lodged of disputes settled.
- The law/legal mandate shall oblige vendors who trade through electronically mediated means to provide the consumer with an opportunity before the completion of a transaction to review a summary of the sales agreement, including the verification and/ or correction of the subjects of the transaction.
- The law/legal mandate shall provide the consumer with the option to void without penalty any contract with a vendor who does not provide an opportunity to review, verify and/ or correct the electronic agreement before the completion of the agreement.
- The law/legal mandate obliges persons who send unsolicited commercial communications to consumers to explicitly provide an option for that consumer to opt-in or opt-out of the receipt of other such communications from that person.

7. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH THE FRAMEWORK OF LIABILITY OF INTERMEDIARIES TO AN ELECTRONIC TRANSACTION

- The law/legal mandate recognizes that there are parties, called intermediaries, who facilitate the electronic transactions between two parties, but themselves are not involved in the subject of the contract. Such persons include telecommunications providers, website hosts, application hosts.
- The law/legal mandate distinguishes the intermediary or telecommunications provider from the parties involved in the transactions through their role as a mere conduit: - a passive agent providing transport, storage or other automatic, technical services which do not modify the content of the electronic document.
- The law/legal mandate makes provision for the exemption of liability of the intermediary from any civil or criminal penalties associated with an electronic document for which it performed no role other than as a mere conduit.
- The law/legal mandate obliges the intermediary to report to the relevant authorities any instance where it believes or has reason to believe that an electronic document for which it is acting as a conduit is in breach of any law.
- The law/legal mandate may identify the relevant record which the intermediary shall produce in the instance where there is an investigation pursuant to its actions with respect to a given electronic document.
- The law/legal mandate provides for the intermediaries' limitation of liability for any civil suit in the instance that in good faith, the intermediary deletes or makes unavailable an electronic document that was stored with its facilities pursuant to an order of the Court, or on obtaining actual knowledge of the illegal activity.
- The law/mandate provides for the intermediary's liability where there is reasonable cause to assume that said party is responsible for the interference of an electronic transmission.

Section II:
Model Legislative Text –
Electronic Transactions

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

Arrangement of Sections

Section III

PART I – PRELIMINARY

Short Title

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

Objective

2. (1) The objectives of this Act are:

a. to eliminate legal barriers to the effective use of electronic records and of electronic communications in commercial transactions;

b. to promote the harmonization of legal rules on electronic transactions across national and/or international boundaries;

c. to facilitate the appropriate use of electronic transactions;

d. to promote business, consumer, and community confidence in electronic transactions; and

e. to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records.

Definitions

3. (1) "Accreditation authority" means the authority empowered to establish norms, regulation and policies for the local public key infrastructure, performing the function of root certification authority, and managing the process of approval ad audit of certification service providers, authentication service providers, and cryptography providers.

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

(3) "Accredited certification service provider" means an entity or a legal or natural person who issues electronic certificates or provides other services related to electronic signatures, which have been accredited by the accreditation authority (accredited certificates).

(4) "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.

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

(6) "Authentication products or services" mean products or services designed to identify the holder of an electronic signature to other persons.

(7) "Authentication service provider"(or authentication authority, or registration authority) means an entity or a legal or natural person whose authentication products or services have been accredited by the Accreditation Authority; performs acknowledgement (authentication) and registration of holders of electronic certificates issued by a certification service provider or by accredited certification service provider, and may resell such certificates under a contract with the latter.

(8) "Certification service provider" means a legal or natural person who issues electronic certificates or provides other services related to electronic signatures.

(9) "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.

(10) "Cryptography provider" means any person who provides or who proposes to provide cryptography services or products.

(11) "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.

(12) "Electronic" means any medium that is 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.

(13) "Electronic agent" means a program, 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.

(14) "Electronic Certificate" means an electronic attestation which links signature-verification data to a person or public body and confirms the identity of that person or public body, or links time-verification data to an electronic record or to an electronic communication and confirm the associated date and time.

(15) "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; or

c. any communication from a tracking device.

(16) "Electronic record" means a set of data that is created, generated, recorded, stored, processed, sent, communicated, and/or received, on any physical medium in or by a computer or other similar device, and that can be read or perceived by a person by means of an information system or other similar device, including a display, print-out or other output of those data. For the purposes of this Act, electronic record refers to information in general, and transaction record (or record of a transaction) refers specifically to transactions (either commercial or non-commercial).

(17) "Electronic signature" means data in electronic form which are attached to, incorporated in or logically associated with other electronic data and which serve as a method of authentication.

(18) "Electronic transaction" means the single communication or outcome of multiple communications involved in the sale or purchase of goods and services conducted over computer-mediated networks or information

systems, where the goods and services may be ordered through such networks or systems but the payment and ultimate delivery of the goods and services may occur without the use of such networks or systems.

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

(20) "Intermediary" with respect to an electronic record, means a person who sends, receives, stores, processes or provides other services with respect to the electronic record for another person, including the provision of content, email, caching and hosting services.

(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 a person acting as an intermediary with respect to that electronic record.

(22) "Public body" means:

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 created, collected, or received in the initiation, conduct or completion of an activity and that comprises content, context and structure to provide evidence or proof of that activity or transaction, being inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in visible and audible form.

(24) "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.

(25) "Telecommunications service provider" means a provider of telecommunications services within the meaning of applicable Telecommunications laws.

(26) "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.

(27) "Transaction" means an action or set of actions relating to the conduct of commercial or non-commercial interactions, between two or more persons, including but not limited to business entities, consumers or

public bodies, such as the sale, lease, exchange, licensing, or disposition of personal property, including goods and intangibles, services, or any combination of the foregoing.

(28) "Transaction record" (or "record of a transaction") means an electronic record reflecting any stage of an electronic commercial or non-commercial transaction.

Exclusions

4. This Act does not apply to:

a. the creation or transfer of any interest in real property;

b. negotiable instruments;

c. documents of title;

d. wills, trusts created by will or any other testamentary instrument;

e. Powers of Attorney;

f. Passports, and Immigration documents;

g. any procedure governed by the Civil Proceedings Rules or by rules of Courts;

h. any class of documents, transactions or laws excluded by Regulation under this Act;

i. any other instrument that may be determined by the Minister by Order.

PART II – ELECTRONIC TRANSACTIONS

Principle of Non-Discrimination

5. Information and transactions shall not be denied legal effect, validity or enforcement solely on the ground that they are represented in electronic form, provided the requirements established in this Act are met.

Prescribed Non-Electronic Form

6. (1) Where any law requires a person to provide information or to enter into a transaction in a prescribed non-electronic form such requirement is satisfied by the provision of the information or the entering into the transaction in an electronic form that is:

a. organized in the same or substantially the same way as the prescribed non-electronic form;

b. accessible to the other person (or to third parties, as the case may be) so as to be usable for subsequent reference; and

c. capable of being retained by the other person (or by third parties, as the case may be).

(2) In subsection (1), providing information includes, but is not limited to, the following:

a. making an application;

b. making, filing or lodging a claim;

c. giving, sending or serving a notification;

d. filing or lodging a return;

e. making a request;

f. making a declaration;

g. filing, lodging or issuing a certificate;

h. making, varying or canceling electronic voting.

(3) Where any law referred to in subsection (1) requires more than one copy of the information or transaction to be submitted to a person, that requirement is satisfied by providing the information or transaction record to the person electronically in accordance with the provisions of this section.

Written Requirements

7. (1) Any law that requires information or transactions to be in writing is satisfied by electronic records if the requirements set forth in Section 6, (1) (b) and (c) hereof are met.

Subsection (1) shall not apply where the interested party consents to waive such requirements.

Signature Requirements

8. (1) Any law that requires a person's signature in relation to any information or transaction is met where the information or transaction is electronically signed, and –

a. a method is used to identify the person and to show the person's approval of the transaction;

b. having regard to all the relevant circumstances when that method was used, including any relevant agreement, the method was reliable as was appropriate for the purposes for which the transaction was entered into;

c. if the signature is required to be given to a public body requires that the method used be in accordance with certain particular technology requirement, the public body's requirement has been met; and

d. if the signature is required to be given to a person other than the public body, that person consents to that requirement being met by using the method mentioned in paragraph (a).

(2) Subject to subsection (3), a digital signature shall be presumed to have satisfied the requirements of subsection (1) (a) and (b) if that signature is –

a. uniquely linked to the person whose signature is required;

b. capable of identifying that person;

c. created by using means that such person can maintain under his sole control; and

d. linked to the transaction to which it relates in such a manner that any subsequent alteration of the transaction is revealed.

(3) Subsection (2) shall not be construed as limiting in any way the ability of any person to:

a. establish in any other manner, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of a advanced electronic signature or other method of indicating identity and approval;

b. adduce evidence of the unreliability of an advanced electronic signature.

(5) In determining whether, or to what extent, an electronic certificate or an electronic signature issued within the jurisdiction subject to this Act is legally effective, no regard shall be had to the geographic location –

a. where an electronic certificate is issued and used; or

b. of the place of business of the certificate service provider or signatory,

- provided the national and/or regional authority in charge of administering the advanced electronic signature system accredits the certificate service provider.

(6) This section shall not affect the operation of any other rule of law that requires –

a. transaction that is entered into electronically to contain an electronic signature (however described);

b. transaction that is entered into electronically to contain an unique identification in an electronic form; or

c. a particular electronic method to be used for transaction that is entered into electronically to identify the originator and to show that the originator approved the transaction entered into.

Acknowledge-ment, Authentication, Notarization, and Verification Requirements

9. Where any law requires an electronic record or signature to be made, acknowledged, authenticated, notarized or verified, by any person, that requirement is met if the following are attached to or logically associated with the electronic record;

a. the advanced electronic signature of that person;

b. in the case of a signature or an electronic record requiring a signature, a statement by that person, attesting to his identity;

c. a statement by that person certifying the performance of all obligations imposed by any other law governing the legal validity of the electronic record; and

d. all other information required to be included under any other law.

Requirement to Produce an Original Document

10. (1) Where any law requires or permits a record of a transaction to be presented in its original form, or to be made available for inspection, that requirement is met where the record of the transaction is produced electronically if:

a. having regard to all the relevant circumstances at the time, the method of electronically producing the record of the transaction provided a reliable means of assuring the maintenance of the integrity of such record;

b. when the record of the transaction or information was sent, it was reasonable to expect that it would be readily accessible so as to be useable for subsequent reference;

c. where the record of the transaction is to be produced to the public body and the public body requires that:

i. an electronic form of the record of the transaction be produced in a particular way, in accordance with particular information technology requirements; or

ii. a particular action be taken to verify receipt of the record of the transaction

the public body's requirement has been met; and

d. where the record of a transaction is to be produced to a person other than the public body, that person consents to the record of the transaction being produced electronically.

(2) For the purposes of subsection (1)(a), the criteria for assessing integrity are:

a. that the record of the transaction has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

b. the purpose for which the record of the transaction is produced; and

c. any other relevant factor.

Keeping Written Documents

11. (1) Where any law requires a person to keep information or record of a transaction for a specified period, that requirement is met by keeping information or record of transaction electronically if the following conditions are satisfied:

a. when the information or record of transaction was first generated in electronic form, it was reasonable to expect that the information or record of transaction would be readily accessible so as to be useable or subsequent reference;

b. having regard to all the relevant circumstances when the information or record of transaction was first generated in electronic form, the method of retaining the information or record of transaction in electronic form provided a reliable means of assuring the maintenance of the integrity of the information or record of transaction that was generated;

c. the traffic data relating to the information or transaction record is also kept in electronic form during the specified period;

d. when the traffic data was first generated in electronic form, it was reasonable to expect that it would be readily accessible so as to be useable for subsequent reference; and

e. if the law requires the information or record of transaction to be kept in electronic form on a particular kind of storage medium, that requirement is met throughout the specified period.

(2) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out is subsection (1) (a) to (e) are met.

Integrity of Information or of Transaction Record

12. (1) For the purposes of sections 10 and 11, the integrity of the information in an electronic record or transaction record is deemed reliable and maintained where the electronic record or transaction record has remained complete and unaltered, apart from:

a. the addition of any endorsement; or

b. any immaterial change,

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

(2) Reliability under subsection (1) shall be determined in light of all the circumstances, including the purpose for which the information, transaction record or electronic record was created.

Recognition of Foreign Documents and Signatures

13. (1) In determining whether or to what extent a foreign information in electronic form or transaction record is legally effective, no regard shall be had to the location where the information or transaction record was created or used, or to the place of business of its creator.

[(2) If the accreditation authority, or a public body empowered to regulate on electronic signatures within the jurisdiction subject to this Act, considers that the policies and practices of a foreign accreditation authority, certification service provider and/or authentication service provider ensure reliability levels at least equivalent to those required in the jurisdiction of the former, it may recognize foreign electronic certificates and authentication services as legally equivalent to the ones accredited by the former].

Electronic Contracts

14. (1) Subject to Part III hereof and unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of an electronic transaction may be expressed:

a. by means of transaction record in electronic form; or

b. by an act that is intended to result in electronic communication, such as touching or clicking an appropriate icon or other place on a computer screen, or by speaking (or, where applicable, by browsing electronic pages which access is allowed under prior express conditions).

(2) An electronic transaction is not invalid or unenforceable by reason only of being in electronic form.

Automated Electronic Contracts

15. (1) An electronic contract may be formed through the interaction of computer program or other electronic means used to initiate an act or to respond to electronic communication, in whole or in part, without review by an individual at the time of the response or act.

(2) The electronic contract formed in accordance with subsection (1) shall be valid and binding provided the contracting party knows or has reason to know that it will cause the device to complete the transaction and the contract terms were capable of being reviewed by the contracting party prior to the formation of the contract.

Effects of Error While Dealing with Electronic Agent

16. (1) An electronic transaction between an individual and an electronic agent's automated source of communication has no legal effect if:

a. the individual makes a material error in electronic communication or in an electronic record used in the transaction;

b. the automated source of communication does not give the individual an opportunity to prevent or correct the error;

c. on becoming aware of the error, the individual promptly notifies the other person; and

d. in a case where consideration is received as a result of the error, the individual returns or disposes of the consideration in accordance with the other person's instructions or in the absence of such instructions takes reasonable steps to return or dispose of the consideration, and does not benefit materially by receiving the consideration.

Expressions of Will

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

Time and Place of Receipt of Electronic Communications

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

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

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

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

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

(4) An electronic communication is deemed to be sent from the sender's place of business and received at the addressee's place of business, unless there is reasonable evidence that the sender has sent the electronic communication from elsewhere.

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

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

Attribution of Electronic Communications

19. (1) An electronic communication is that of the person who sends it, if it is sent directly by the person or by an electronic agent on his behalf. As between the originator and the addressee, an electronic record shall be attributable to the originator if it was sent:

a. by a person or his electronic agent or by another person who had been authorized by the originator to send the electronic record on his behalf; or

b. by the originator's electronic agent.

(2) As between the originator and the addressee, an addressee shall be entitled to attribute an electronic record to the originator, and to act on that assumption, if:

a. in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

b. the electronic record as received by the addressee resulted from the actions of a person whose relationship with the originator, or with any agent of the originator, enabled that person to gain access to a method used by the originator to identify electronic records as his own.

(3) Subsection (2) shall not apply

a. as of the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly; or

b. in a case to which subsection (2)(b) applies, at any time when the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator.

4) The addressee shall be entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that it duplicates another electronic record and the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, the electronic record was a duplicate.

Other rules of Law Not Affected

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

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

Consent

21. (1) Nothing in this Act requires a person to use, provide or accept transaction records without consent.

(2) Nothing in this Act shall:

a. require any person to use or accept electronic communications, electronic signatures, or electronic contracts; or

b. prohibit any person engaging in a transaction through the use of electronic means from:

i. varying by agreement any provision relating to legal recognition and functional equivalency of electronic communications, signatures, and contracts; or.

ii. establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

(3) This Act applies to any transaction between parties each of whom has agreed to conduct the transaction electronically.

(4) The fact as to whether or not a party agrees to conduct a transaction electronically shall be determined:

a. where the party is a public body, by express stipulation of the public body, made accessible to the public or to those most likely to communicate with it for particular purposes;

b. in the case of any other party, by the context and surrounding circumstances including the party's conduct.

(5) A party that agrees to conduct a particular transaction electronically may refuse to conduct other transactions electronically.

22. (6) The parties to an electronic commercial transaction may specify that a particular certification and/or authentication service provider or certain class of certificates shall be used in connection with electronic records or signatures submitted to them.

PART III – CONSUMER PROTECTION

Required Data

23. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following data available to consumers in a clear and comprehensible manner:

a. the full name and legal status;

b. its physical address and telephone number;

c. its web site address and e-mail address;

d. the physical address where the supplier will receive legal service of documents;

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

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

g. the method of payment;

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

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

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

k. the return, exchange, insurance and refund policy of the supplier;

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

m. a channel for receipt of notices from the consumer, in the same area of the electronic communication originally used by the supplier to display the offering and/or to promote the transaction.

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

a. to review the entire electronic transaction;

b. to correct any mistakes; and

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

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

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

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

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

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

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

(7) The supplier shall ensure the availability of an automated response system to acknowledge receipt of electronic communications sent by the consumer.

(8) A consumer electronic transaction shall be deemed concluded upon receipt by the consumer of the electronic communication from the supplier confirming receipt of consumer´s acceptance of the offering.

Cool-Off Period

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

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

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

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

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

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

a. for financial services, including investment services, insurance and reinsurance operations, and banking services;

b. conducted as an auction;

c. for services which began, with the consumer's consent, before the applicable cooling-off period specified in subsection (1);

d. where the price for the supply of the goods, services or facilities in question is dependent on fluctuations in the financial markets and cannot be controlled by the supplier;

e. where the goods in question:

i. are made to the consumer's specifications;

ii. are clearly personalized;

iii. by reason of their nature cannot be returned; or

iv. are likely to deteriorate or expire rapidly;

f. where audio or video recordings or consumer software are unsealed by the consumer;

g. for the sale of newspapers, periodicals, magazines or books;

h. for the provision of gaming or lottery services; or

i. for the provision of accommodation, transport, catering or leisure services or facilities, which the supplier undertakes to provide (when the transaction is concluded) on a specific date or within a specific period.]

Unsolicited Commercial Messages

25. (1) A person who sends unsolicited commercial communications to consumers shall limit the scope of addressees to the ones who have evidenced potential interest in the subject matter of the communication, to be clearly disclosed in the title of the communication, and give to a consumer to whom any communications is sent:

a. the opportunity to decline to receive any further such communications from that person and provide a valid electronic address for such purpose; and

b. upon request by the consumer, the identifying particulars of the source from which that person obtained consumer's information or other personal information.

(2) A person who fails to comply with subsection (1) commits an offence and is liable on summary conviction to a fine of not less than …… (dollars) for the first conviction and of not less than ….. (dollars), each, for any subsequent conviction.

PART IV – INTERMEDIARIES AND TELECOMMUNICATIONS SERVICES PROVIDERS

Liability

26. (1) An intermediary or telecommunication services provider who merely provides a conduit for the transmission of electronic communication shall not be liable for their contents if such intermediary or telecommunication service provider has no actual knowledge or is not aware of facts that would, to a reasonable person, indicate a likelihood of criminal liability or liability for a tort in respect of material on the Internet or who, upon acquiring actual knowledge or becoming aware of such facts, do not proceed as per section 26 hereof, as long as it:

a. does not initiate the transmission;

b. does not select the addressee;

c. performs the functions in an automatic, technical manner without selection of the electronic record; and

d. does not modify the electronic record contained in the transmission.

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

a. for the sole purpose of carrying out the transmission in the information system;

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

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

(3) An intermediary or telecommunications service provider is not required to monitor any information contained in an electronic record in respect of which the intermediary or telecommunications service provider provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

(4) Nothing in this section relieves an intermediary or telecommunications service provider from complying with any court order, injunction, writ, ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic record or of an electronic communication or transaction.

Procedure for Dealing with Notice of Unlawful Actions

27. (1) If an intermediary or telecommunication services provider has actual knowledge that the data in an electronic record or electronic communication gives rise to criminal liability or liability for a tort or that may be reasonably believed to give rise to criminal liability or liability for a tort, and has obtained from the user of its services information which can not reasonably indicate otherwise, the intermediary or telecommunication service provider shall as soon as practicable:

a. notify appropriate law enforcement authorities of the relevant information, where required by criminal laws in effect;

b. where authorized by written law, disclose the identity of the person for whom the intermediary or telecommunications service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary; and

c. where authorized by written law, remove the information or data message from any information processing system within the intermediary's or telecommunications service provider's control and cease to provide or offer to provide services in respect of that information or take any other action authorized by law.

(2) Failure to disclose knowledge of unlawful content under subsection (1) above constitutes an offence.

Offer of Goods and Services in Safe Environment

28. (1) The supplier of the electronic offering of goods and services shall ensure that such services are carried out in a reasonably safe electronic environment, and that such safety conditions are publicly disclosed.

(2) Any breach of security which may affect the confidentiality of consumer´s private data shall be immediately informed by the supplier to the consumer, at the electronic address provided by the consumer for contact purposes.

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

INTRODUCTION

1. This legislative text develops a legal framework for electronic transactions ("e-transactions"). The main objectives of this model legislative text are to eliminate legal barriers to electronic commerce ("e-commerce"), harmonize legal rules concerning national or international e-transactions, promote confidence on the e-commerce, and facilitate electronic filing of documents with the government and electronic delivery of government services ("e-government").

2. These explanatory notes are aimed to explain the contents of this model legislative text, and shall be read in conjunction with it. They explain the importance of key provisions of this model legislative text and, where applicable, call attention to particular discussions held by the HIPCAR[8] Working Group[9], highlighting different options of regulation discussed therein. They are not, and are not meant to be, a detailed description of this legislative text. 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 on some particular provision, no detailed explanation is given.

3. This model legislative text (Act) consists of four parts**:**

   - **Part I** outlines the objectives of this Act, provides definitions on the applicable terminology, and excludes certain matters from application of this legislative text;
   - **Part II** contemplates the principle of non-discrimination against electronic information and transactions, establishes formal requirements applicable to electronic transactions, provides criteria for determining integrity of electronic information or of transaction record, as well as for recognition of foreign electronic documents and signatures, addresses automated electronic contracts and electronic agents, defines time and place of receipt of electronic communications, sets forth rules for attribution of electronic communications, and acknowledges the need of consent from interested parties;
   - **Part III** establishes the obligation of suppliers to provide certain data to consumers of electronic offerings of goods or services, guarantees a "cool-off" period for consumer's cancellation of electronic transactions and related credit agreements, and defines requirements for the sending of unsolicited commercial messages;

---

8 The full title of the HIPCAR project is *"Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures".* This 3-year project was launched in September 2008, within the context of an umbrella project embracing the ACP countries funded by the European Union and the International Telecommunication Union. The project is implemented by the International Telecommunication Union (ITU) in collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU).

9 The members of the HIPCAR Working Groups include Ministry and Regulator representatives nominated by their national governments, relevant regional bodies and observers – such as operators and other interested stakeholders. The Terms of Reference for the Working Groups are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.
The Second Consultation Workshop (Stage B) for HIPCAR Working Group 1 on ICT Legislative Framework – Information Society Issues was held in Barbados, 23-26 August 2010. Participants reviewed, discussed and adopted by broad consensus the Draft Model Legislative Text on the respective area of work. Where ever the word "working group" appears in this document, it refers to the aforementioned Workshop. The word "beneficiary country" in this document refers to the 15 ACP countries in the Caribbean region identified under the ITU/EU-funded HIPCAR project.

- **Part IV** regulates on liability of intermediaries and of telecommunications services providers, establishes a procedure for dealing with notice of unlawful actions, and requires that supplies ensure safe environment for the electronic offering of goods and services.

COMMENTARY ON SECTIONS

PART I – PRELIMINARY

4. Part I provides short title and commencement clause in Section 1, objectives in Section 2, and definitions in Section 3.

   Part I has motivated a discussion within the HIPCAR Working Group with regard to the drafting style in different jurisdictions. It was discussed whether it should include a Section outlining the objectives of this model legislative text. Consensus reached was that such question shall be left to the discretion of beneficiary states.

Section 2. Objectives

5. Section 2 lists the objectives of this model legislative text (Act), which are primarily targeted at fostering e-commerce, but may extend (at least, in general terms) to other sorts of electronic transactions and to e-government.

Section 3. Definitions

6. The definition of **computer** provided by subsection (9) leaves room for encompassing any electronic device which may perform functions typical of computers.

7. There was a debate within the HIPCAR 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, makes it advisable to maintain broad wording mentioning "electronic information or communication devices" in addition to the references to "computer" and to "computer devices".

8. **Data** is defined in subsection (11) as representing facts, information, or concepts in a form suitable for processing in an information system.

9. Data was selected as defined expression in lieu of "information", which is an expression present in some countries' legislation relating to general transactions, not specifically to electronic transactions. As the scope of this Act solely comprises electronic transactions, the intent here was to mean only the facts, information, and concepts which have been represented in electronic, binary digits form.

10. The HIPCAR Working Group debated the convenience of including the expression "state" in the definition of "data", which would purport to emphasize that data may not only be logically conceived as sequences of "0" and "1" digits (which sequences represent letters or numerals), but also mean the tangible change of electromagnetic or optical status in a computer which the information system "reads" as 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 legally qualify data as "thing" (implying, for instance, that it may be subject to possession or to misappropriation), 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 states.

11. 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 national and international levels, therefore their equivalency is established 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 as to facilitate common interpretation and effective enforcement.

12. The automated electronic response used as interface for interaction of human beings with computers characterizes the **electronic agent** as defined in subsection (13). 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.

13. The definition of **electronic communication**, contained in subsection (15), focuses on the transfer of records, including the respective sending and receipt (while the definitions of "computer" and of "information system" are limited to focus on the internal activities performed by the computer or by the information system).

14. The HIPCAR Working Group discussed the convenience or not of including references to "any wire or oral communication" and to "any communication from a tracking device". Some concern was voiced to the effect that such expressions might overlap with expressions already existing in telecommunications laws of certain countries, especially with regard to telephony, paging, and tracking devices. The Working Group decided that it shall be left to the discretion of beneficiary states whether to maintain such wording or not.

15. Subsection (16) 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.

16. 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.

17. The distinction between those complementing expressions – "data", and "electronic record" – is necessary for legislating on e-transactions since the manifestation of consent or 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).

18. 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 legislative text within the wording "electronic information or communication devices"), as the latter is clearly intended to mean a device used by human beings to access/perceive electronic records.

19. 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 e-transactions, extending it beyond traditional media in order to comprise, for instance, biometrical media (such as scanned image of fingers, of the face, or of the iris), which may be increasingly applied in the context of e-transactions (as it has started to happen with banking automated teller machines in some countries).

20. 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 externally to it.

21. Finally, such subsection clarifies that the concept of "electronic record" has been used throughout this legislative text to mean information in general, while the concepts of "transaction record" (or of "record of a transaction") have been used specifically with regard to transactions (either commercial or non-commercial).

22. **Electronic signature** has been defined in subsection (17) as a method of authentication. In conjunction with relevant definition of additional, relating expressions (such as **Accreditation authority, Accredited certificate**, **Accredited certification service provider**, **Advanced electronic signature**, **Authentication products and services**, **Authentication service provider**, **Certification**

service provider, **Cryptography provider**, **Electronic Certificate**, and **Signature**) featured in other subsections of Section 3, it provides coherent meaning to a key system of validation of e-transactions – the system of authentication, certification, and accreditation of digital signatures – capable of identifying authorship, origin, time, and other elements of electronic records.

23. The definitions adopted for such set of expressions have taken into account that the beneficiary state may or may not have implemented a system of certification services for 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 structures of roles and powers, the allocation of regional and/or national resources, the offering of time-stamping certification services, and so on).

24. By taking such approach, the definition on electronic signatures facilitates integration with other provisions of this legislative text (such as the ones relating to signature requirements and to production of an original document) since the generic wording adopted provides flexibility to accommodate different manners of using electronic signatures to sign a document and guarantee its integrity.

25. Equally important for understanding the phenomena surrounding e-transactions is the definition of **information system**, contained in subsection (19). While "computer" means single electronic equipment, "information system" comprises groups of inter-connected devices, typical of electronic networks.

26. The broad definition of "information system" comprehends networks at various levels, including the Internet, which is technically considered a "network of networks". Given the magnitude of the Internet as technological platform for e-transactions, a specific reference was made to it. The concept of group of inter-connected devices is comprehensive enough to include any equipment linked to the Internet.

27. The HIPCAR Working Group also debated on whether this model legislative text should use the expression "information system" rather than the expression "computer system". The fact that "information system" (and "information-processing system") has been the expression 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 for the context of e-transactions, therefore the Working Group has opted to use "information system", while adding "computer system" as equivalent expression. The level of technical accuracy wished for addressing such concepts in this legislative text was left to the discretion of beneficiary states.

28. The definition of **intermediary**, contained in subsection (20), is broad enough to encompass access, content, and hosting Internet services providers, as well as possible other services providers.

29. The concept of **originator**, as defined in subsection (21), comprises not only the person who actually sends an electronic communication but also the person who instructs another to send on his behalf and the person who uses an electronic agent for sending.

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

31. The HICPAR Working Group decided to include a remark to the effect of clarifying that "electronic agent" does not include persons acting as "intermediaries" (which expression was defined in subsection (20)) with respect to the electronic record.

32. **Public body** is defined in subsection (22) as including any ministry or department, wholly or partially owned state companies or enterprises, bodies exercising statutory authority of legislative, executive or judicial nature, and sub-national or local public authorities, including municipalities.

33. Such definition is in line with the observation in topic 23 above, which mentions the possibility of further regulation establishing a system of authentication and/or certification of digital signatures. The issue here is that e-transactions present 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, is quite large, which justifies that such definition be so comprehensive.

34. The definition of "public body" is used in a large number of provisions of this legislative text (for instance, Sections 8.(1).c, 10.(1).c and .d, 13.(2), and 21.(4).a). In addition, it pre-establishes the large scope of "public bodies" expected to issue or to be beneficiary of further regulation, providing consistency for the issuance of subordinate legislation.

35. Subsection (26) addresses **traffic data** aiming to comprise data which qualify the flow of any given electronic communication. Details such as origin, route, destination, date, time, size, and duration are very important for determining authorship, place, and time of certain transactions (especially, where electronic communication flows split by "packages" which may follow different paths up until reaching their intended destination, as in the Internet).

Section 4. Exclusions

36. Although this model legislative text purports to apply to a wide scope of transactions (either commercial or non-commercial, entered into by and between private and/or public parties), there are situations which can not or should not be subject to its provisions. Section 4 brings a list of such situations, which includes: i) creation or transfer of interests in real property, ii) negotiable instruments, iii) documents of title, iv) wills, trusts created by will or other testamentary instruments, v) Powers of Attorney, vi) passports and immigration documents, vii) any procedure governed by the Civil Proceedings Rules or by rules of Courts, viii) any class of documents, ix) transactions or laws excluded by Regulation under this Act, and x) any other instrument that may be determined by the Minister by Order. The purpose of this Section is mainly to avoid any conflict with other Laws.

PART II – ELECTRONIC TRANSACTIONS

Section 5. Principle of Non-Discrimination

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

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

Section 6. Prescribed Non-Electronic Form

39. The philosophy behind prescription of form to information or to transactions is to ensure proper levels of reliability. Such philosophy can also be addressed by information or transactions in electronic form. This Section lists the criteria which determine such equivalence: i) organization in the same or substantially the same way as the prescribed non-electronic form, ii) accessibility to other persons so as to be usable for subsequent reference, and iii) capability of being retained by other persons.

40. This Section is in line with the internationally accepted principle of functional equivalence, which determines that no restriction shall be imposed on the on-line environment which is not also imposed in the off-line universe. The equivalence established by this Section fits the purpose of bridging electronic and non-electronic requirements, facilitating migration to the digital environment.

41. The HIPCAR Working Group discussed the possible implications of the criterion which requires capability of retention, which may overlap with data retention and privacy laws, or with contractual arrangements for hosting or warehousing services. Although the wording used for such requirement is quite generic (i.e., has not stipulated term for retention, and has allowed that retention be performed by third parties), beneficiary states shall verify whether such requirement conflicts with any other legal provision, and establish rule of precedence, where applicable.

42. Subsection (2) lists examples of situations where the electronic provision of information shall be deemed equivalent to the non-electronic provision of information. One of the situations listed refers to making, varying or cancelling "electronic voting", which is intended to address electronic general elections (as voting in political elections or in some other elections has progressively become an electronic process, to certain extent, notwithstanding most relevant legislation do not refer to it). The HIPCAR Working Group has noted that some countries of the region in the Caribbean may wish to remove such item, where it overlaps with Representation of the Peoples Act or with similar legislation.

Section 7. Written Requirements

43. Similarly to what happens to prescribed form, written requirements may refer both to electronic and to non-electronic information or transactions.

44. Compliance with the principle of functional equivalence presupposes establishing criteria which may bridge electronic and non-electronic requirements for written information or transactions.

45. For the sake of consistency, this Section has reported to criteria established in Section 6 (more specifically, to the ones contemplated in its items 1.(b) and .(c)).

46. This Section also provides for waiver of those requirements should the interested parties consent to it.

Section 8. Signature Requirements

47. The principle of functional equivalence shall also apply to signature requirements.

48. Section 8 establishes criteria which bridge requirements for electronic and for non-electronic signatures. Those cumulative criteria include: i) a method to identify the person and show his approval of the transaction; ii) the method was reliable and appropriate for the purposes of the transaction; and iii) compliance with technology requirements imposed by public bodies, where applicable.

49. Subsection (2) specifically addresses digital signatures, establishing presumption that they satisfy the requirements of a reliable and appropriate method to identify a person and to show his approval of the transaction where the digital signature is: i) uniquely linked to the signatory; ii) capable of identifying the signatory; iii) maintained under control of the signatory; and iv) linked to the transaction in a way to reveal any alteration of it.

50. Those generic criteria are important since digital signatures are associated with different levels of security, while the intent of this model legislative text is not to impose restrictions which could impair compliance with the internationally accepted principle of technological neutrality, according to which there shall be no unreasonable preference for particular technologies.

51. Subsection (3) refers to advanced electronic signatures, allowing that any person establishes their reliability or adduces evidence on their unreliability in a manner different than the ones set forth in subsections (1) and (2).

52. This subsection is important as advanced electronic signatures provide own presumption of reliability, irrespectively of any other factors, and such presumption is expected to be enforced (or challenged, if necessary).

53. Subsection (5) contemplates electronic certificates or electronic signatures issued within the jurisdiction subject to this legislative text, establishing that no regard shall be had to geographic location, provided the national and/or regional authority in charge of administering the advanced electronic signature system accredits the certificate service provider.

54. This subsection is important as it creates the possibility that certificates accredited by a possible regional authority be legally effective in the beneficiary state.

55. Of course, this legislative text does not purport to create any regional authority, but it anticipates such hypothesis, which may be convenient to the extent it is plausible and wished.

56. Subsection (6) states that this Section shall not affect the operation of any other rule of law which requires that a transaction contain an electronic signature, an unique identification, or a particular method to identify the originator and to show his approval of the transaction.

57. This subsection is important as it avoids or reduces the likelihood of conflict with any related laws, such as the ones which impose identification through other means (such as biometrical) or which determine that every transaction be given a unique number (as in the case of electronic tax invoices).

Section 9. Acknowledgement, Authentication, Notarization, and Verification Requirements

58. Following the path of building legal equivalence between electronic and non-electronic records or signatures, Section 9 establishes the criteria pursuant to which requirements of acknowledgement, authentication, notarization or verification are met where electronic records and signatures are concerned.

59. Those criteria include: i) advanced electronic signature; ii) statement by signatory attesting his identity; iii) statement by signatory certifying performance of all obligations relating to validity of the electronic record; and iv) all other information required to be included under any other law.

60. This Section is important as it provides a number of options for satisfying said requirements, including non-electronic alternatives, which may be particularly convenient where advanced electronic signatures are not available, or are too expensive or bureaucratic under the circumstances, or where social digital inclusion has not reached interested parties.

Section 10. Requirement to Produce an Original Document

61. Although it is notorious that electronic records present some technical difficulties for determining which the original of a record is and which is a copy of it, there are ways which may support equivalence to production of non-electronic original documents.

62. Section 10, in its subsection (1), lists criteria of equivalence with electronic records of a transaction. Those criteria include: i) existence of a reliable means of assuring integrity of the record; ii) records sent be readily accessible to be useable for subsequent reference; iii) particular requirements imposed by public bodies are satisfied; and iv) consent of the interested person to the record being produced electronically.

63. Such provision is important as it complies with the principle of functional equivalence, as well as provides reasonably available options to establish original electronic records of a transaction.

64. Subsection (2) clarifies how an assessment on the integrity of a record may be accomplished. To that effect, it establishes the following criteria: i) the record remains complete and unaltered (apart from changes arisen in the normal course of communication, storage or display); ii) purpose of production of the record; and iii) any other relevant factor.

65. This subsection is important as it ensures flexible assessment on the integrity of a record by taking into consideration the purpose of production of the record and any other relevant factor.

66. Not least important, it disregards immaterial changes (to the record) which are due to normal causes; as digital environments are often subject to change (for technological update, or for other reasons), immaterial, normal changes shall not affect the status of "complete" and "unaltered" of a record.

Section 11. Keeping Written Documents

67. Section 11, in subsection (1), outlines the criteria which satisfy requirements of keeping written documents, where electronic records of a transaction are concerned. Such criteria include: i) it was reasonable to expect that the information or record would be readily accessible so as to be useable for subsequent reference; ii) the method of retaining information or record has provided reliable means of assuring integrity; iii) traffic data is also kept, iv) it was expected that traffic data would be readily accessible so as to be useable for subsequent reference; and v) compliance with possible legal requirement of keeping the information or record on a particular kind of storage medium. Subsection (2) allows that the above requirements are met using the services of any other person.

68. This Section is important as it contemplates practical ways for meeting requirements of keeping electronic information or records.

69. It is worth noting the presence of traffic data amongst the criteria selected, which points to the convenience of keeping not only "contents" of an information or record but also the data associated with its sending or receipt. The traffic data may be a key element for recognition of electronic information or records.

Section 12. Integrity of Information or of Transaction Record

70. Section 12 complements the provisions of Section 10 by extending to electronic information the criteria it provides for assessment of integrity in the context of production of original documents.

71. It also complements Section 11, extending such criteria to assessment of integrity in the context of keeping written documents.

72. The importance of this Section is that it guarantees consistency for the assessment of integrity of electronic information and records in both contexts.

Section 13. Recognition of Foreign Documents and Signatures

73. Similarly to the provisions of Section 8.(5) relating to legal effects of electronic certificates or of electronic signatures issued within the jurisdiction subject to this Act (see topic 48 above), Section 13 deals with recognition of foreign documents and signatures, establishing, in subsection (1), that no regard shall be had to the location where the information or transaction record was created or used, or to the place of business of its creator.

74. This Section is particularly important for the reason that subsection (2) authorizes the accreditation authority, or a public body empowered to regulate on electronic signatures within the jurisdiction subject to this legislative text, to recognize foreign electronic certificates and authentication services where it considers that the foreign country has policies and practices as reliable as the ones required in the jurisdiction of the former.

75. This provision may be of interest assuming a beneficiary state has defined, or intends to define, its own policies and practices on authentication, certification, and on accreditation services, and wishes to establish equivalence with the ones in effect in other countries, based on such comparison.

76. Also important to mention, such provision is not exclusively applicable to countries which have already created an accreditation authority, as it mentions the possibility that the judgment on equivalence with other countries' policies and practices be performed also by a public body empowered to regulate on electronic signatures.

77. The HIPCAR Working Group called the attention to the possible convenience of beneficiary states establishing policy or regulations on accreditation of the root certificate by foreign entities. This may be another item for comparison with other countries in the judgement on equivalence of relevant policies and practices.

Section 14. Electronic Contracts

78. Section 14 establishes general principles regarding admissibility of electronic contracts.

79. Subsection (1) allows that the formation or operation of an electronic transaction be expressed: i) by means of transaction record in electronic form; or ii) by an act intended to result in electronic communication.

80. Item ii) above provides examples of acts intended to result in electronic communications, quoting "touching or clicking an appropriate icon or other place on a computer screen, or by speaking (…)".

81. This wording is important as it makes clear that most recent forms of electronic contracting (such as the so-called "web-wrap agreements") are also admissible.

82. Item ii) additionally refers to the so-called browse wrapping agreements ("or, where applicable, by browsing electronic pages which access is allowed under prior express conditions)".

83. Specifically in this regard, the HIPCAR Working Group has considered that browse wrapping agreements may not be enforceable under some circumstances, therefore it has decided that maintenance of this item shall be up to the discretion of beneficiary states.

84. Subsection (2) states that an electronic transaction is not invalid or unenforceable for the single reason that it is in electronic form. This reinforces the general principle on admissibility of electronic contracts.

Section 15. Automated Electronic Contracts

85. Section 15, in subsection (2), establishes that automated electronic contracts are valid and binding, provided: i) the contracting party knows or has reason to know that it will cause the device to complete the transaction; and ii) the contract terms were capable of being reviewed by the contracting party prior to the formation of the contract.

86. As automated electronic contracts imply interaction of the consumer with an electronic device which is not necessarily able to answer any questions the consumer may have, consent of the consumer shall be a point of concern, and be protected as per the provisions of this Section.

Section 16. Effects of Error while Dealing with Electronic Agent

87. Interactions with electronic agents are subject to errors which may impair the validity of an electronic transaction. Section 16 determines that in such event the electronic transaction has no legal effect, if: i) the individual makes a material error; ii) the individual is not given opportunity to prevent or correct the error; iii) the individual promptly notifies about the error once becomes aware of it; and iv) the individual returns consideration received as a result of the error.

88. This Section is important as it protects individuals against failures in electronic contracting via electronic agents. Such provision is welcome as a large number of web sites seem not to be prepared to handle complaints by consumers which had problems in contracting interfaced by electronic agents.

Section 17. Expressions of Will

89. Section 17 establishes the general admissibility of declarations of will or of other statements communicated via electronic means.

90. It circumscribes its effects to the relationship between the originator and the addressee of that communication.

91. Such limited scope does not impair the provision of Section 4.(d) which excludes wills from application of this model legislative text.

Section 18. Time and Place of Receipt of Electronic Communications

92. Time and place are of the essence of transactions, inclusively where the transaction is entered into in electronic form. Therefore, special attention shall be paid to the determination of the moment and location of sending or of receipt of a relevant electronic communication.

93. Subsection (1) establishes that an electronic communication is sent when: i) it enters an information system outside the sender's control, or, if the sender and the addressee use the same information system, ii) when it becomes capable of being retrieved and processed by the addressee.

94. The HIPCAR Working Group decided to leave item ii) up to the discretion of beneficiary states, as each country has its own legal policies regarding contracting in general, which may extend to electronic contracting.

95. The rationale for keeping item ii) prioritizes the interest of the addressee, while the rationale for eliminating it prioritizes the interest of the sender. Therefore, this is typically an issue of legislative policy, to be resolved by beneficiary states.

96. Subsection (2) mirrors the provisions of subsection (1) by establishing the moment of receipt of an electronic communication and by mentioning the criteria of capability to retrieve and process the electronic communication. Therefore, the observations made in topics 94 and 95 above shall apply to subsection (2) as well.

97. Subsection (3) allows that the parties agree otherwise regarding the provisions of subsections (1) and (2).

98. This is important as the free negotiation between the parties may overcome different legislative policies on the matter, especially where the electronic transaction is entered into by and between parties subject to different jurisdictions.

99. Subsection (4) determines the place of sending and of receipt of electronic communications, prioritizing the criteria of place of business of the parties.

100. Subsections (5) and (6) establish subsequent criteria applicable in the event a sender or an addressee has more than one place of business or has none. In such situations, the place considered shall be, consecutively, i) the one with closest relationship with the underlying transaction, or ii) the person's principal place of business, or iii) the person's place of habitual residence.

101. This provision is important as in many electronic transactions, especially the ones entered into web sites, it is hard to find the actual address of a sender or of an addressee, and subsections (4) through (6) provide practical ways to overcome such difficulty.

Section 19. Attribution of Electronic Communications

102. Given the fact that electronic communications facilitate the sending or receipt via third parties, as well as anonymous communications, the matter of attribution requires careful regulation.

103. Subsection (1) establishes that, as a general rule, an electronic communication is that of the person who sends it, where it is sent directly by the person or by an electronic agent on his behalf.

104. It also establishes that an electronic record shall be, within the relationship between the originator and the addressee, attributable to the originator where it was sent: i) by a person authorized by the originator or by the electronic agent of such person; or ii) by the originator's electronic agent.

105. This subsection is important as it attributes to the originator virtually all, or almost all, possible situations where the electronic communication was sent, directly or indirectly, by the originator or on his behalf.

106. Subsection (2) deals with situations where the addressee can attribute certain electronic communication to the originator. This is allowed where: i) the addressee properly applies a procedure previously agreed to by the originator for such purpose; or ii) the electronic record received by the addressee resulted from action of a person which relationship with the originator or with his agent enabled that person to gain access to a method used by the originator to identify electronic records as his own.

107. This subsection is important as it entitles the addressee to effectively attribute electronic communications to the originator, based on initiatives which may be available to the addressee.

108. Subsection (3) excludes the possibilities granted addressee by subsection (2), where: i) an addressee receives notice from the originator disclaiming that the communication is not his or hers, or ii) where an addressee knew or should have known that the electronic communication was not of the originator's.

109. Those exclusions seem reasonable as they are justified by situations where good faith of the addressee could hardly be evidenced.

Section 20. Other Rules of Law Not Affected

110. Section 20 avoids or reduces the chances of conflict of laws by establishing that nothing in this legislative text shall limit the operation of any other law that: i) expressly authorizes, prohibits or regulates the use of transaction records, including a method of electronic or advanced electronic signature; or ii) requires a record of transaction to be posted or displayed in a specific manner, or requires a record of transaction to be transmitted by a specific method.

111. This section is important as it guarantees that specific situations where electronic signatures or where records of transactions are concerned can be treated in conformity with their specificity. As this legislative text purports to provide general guidelines and rules regarding electronic transactions, it shall ensure an opening so that specific situations are framed by other laws or regulations.

Section 21. Consent

112. Section 21 establishes the general principle that no one is required to use, provide, or accept transaction records (electronic, as per the definition found in Section 3.(28)), electronic communications, electronic signatures, or electronic contracts without consent. This provision is in line with principles of freedom of will and of freedom of economic initiative.

113. Subsection (2) determines that any person engaging in such transactions is entitled to: i) vary by agreement any provision relating to legal recognition or to functional equivalence of electronic communications, signatures, or contracts; and ii) establish reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

114. This subsection is important as it provides opportunity for balancing electronic contracting.

115. Subsection (4) states that the agreement of a party to conduct a transaction electronically shall be determined: i) where the party is a public body, by express stipulation made available; and ii) in the case of any other party, by the context and by surrounding circumstances, including the party's conduct.

116. This provision is important as it acknowledges the difference which shall apply where requirements for public or for private parties are concerned, and because it opens for considering a great deal of factors where the party is not a public body.

117. Subsection (6) states that in electronic commercial transactions the parties are free to specify particular certification and/or authentication service provider or certain class of certificates to be used in connection with electronic records or signatures.

118. This provision recognizes the specific situation of commercial transactions, where the balance between the parties may depend on agreement on the use of particular services to enhance security of the contracting process.

PART III – CONSUMER PROTECTION

Section 22. Required Data

119. Section 22 brings, in subsection (1), a long list of data to be provided by suppliers to consumers who have entered into an electronic transaction of sale, hiring, or exchange of goods or services. Such data, which shall be provided in a clear and comprehensible manner, include, among others: i) full name and legal status; ii) physical address and telephone number; iii) web site address and e-mail address; iv) physical address where a supplier will receive legal service of documents; v) supplier's security procedures and privacy policy; and vi) a channel for receipt of notices from the consumer in the same area of the electronic communications originally used by supplier to display the offering and/or to promote the transaction.

120. This subsection is important as it helps overcome the information gap between suppliers and consumers, which is quite common in the digital environment, where it is sometimes disguised by the appearance of trust that web sites intend to inspire.

121. Subsection (2) determines that suppliers provide consumers with opportunity to: i) review the entire electronic transaction; ii) correct any mistakes; and iii) withdraw from the transaction before finally placing any order.

122. This subsection is important as it gives consumers proper opportunity to review, fix, or cancel his consent to a transaction.

123. Subsection (3) states that if supplier fails to comply with the obligations set forth in subsections (1) and (2), the consumer may cancel the transaction within fourteen days of receiving the goods or services.

124. This subsection is important as it ensures the right for consumers to terminate the transaction for cause.

125. Subsection (4) complements the provisions of subsection (3) by establishing the consequences of cancellation of the transaction as per the latter. Such consequences are: i) consumer shall return the goods, or cease using the services; and ii) supplier shall refund all payments, inclusively the cost of returning the goods.

126. Subsection (5) imposes on supplier the obligation to utilize a secure payment system, considering technological standards and the type of transaction.

127. This subsection is important as it protects consumers against frauds which may take place due to unsecure payment systems selected by suppliers. Such protection is enhanced by subsection (6), which confirms supplier's liability for damages.

128. Subsection (7) states that supplier must ensure availability of an automated response system to acknowledge receipt of electronic communications sent by consumer.

129. This provision is important as it protects consumers from delays, or from denial by supplier about receipt of consumer's communications (inclusively, about receipt of purchase orders sent by consumers, or of acceptance of web-wrap offerings).

130. The provisions of this model legislative text, which regulate the sending or receipt of electronic communications, shall apply in conjunction with this subsection where they do not conflict, otherwise this subsection shall prevail as it provides more specific protection, to more vulnerable parties.

131. Subsection (8) establishes that an electronic transaction shall be deemed concluded upon receipt by consumer of supplier's electronic communication confirming receipt of consumer's acceptance of the offering.

132. This subsection is important as it protects the consumer from the supplier's allegation that failure to comply with the offering was due to that the supplier has not received the consumer's acceptance of the offering, which event is difficult or even impossible for consumers to inspect.

133. The provision of subsection (8) calls attention to a comment raised by the HIPCAR Working Group in the sense that beneficiary states shall verify whether the provisions contained in Part III are compatible with more general consumer protection laws in effect in the jurisdiction of beneficiary states.

Section 23. Cool-Off Period

134. Section 23 regulates the events which entitle the consumer to cancel without reason and without penalty any transaction and any related credit agreement within seven days from the receipt of goods or from conclusion of a services agreement.

135. Subsection (2) establishes that the only charge which may be levied on the consumer is the direct cost of returning the goods.

136. Subsection (3) determines that where payment for goods or services was made prior to the cancellation of the transaction, the consumer is entitled to full refund within thirty days of the date of cancellation.

137. Subsection (4) lists the electronic transactions excluded from application of this Section, namely: i) financial services; ii) transactions conducted as an auction; iii) services which began before the cooling-off period; iv) transactions which prices fluctuate according to the financial markets and cannot be controlled by supplier; v) goods which are made by order, are clearly personalized, cannot be returned, or are likely to deteriorate or rapidly expire; vi) audio or video recordings or consumer software unsealed by consumer; vii) newspapers, periodicals, magazines or books; viii) gaming or lottery services; and ix) accommodation, transport, catering or leisure services or facilities.

138. This subsection is important as the above referenced goods and services actually do not justify cooling-off period or cancellation of the transaction.

Section 24. Unsolicited Commercial Messages

139. Section 24 protects consumers from receipt of abusive unsolicited commercial messages.

140. Subsection (1) establishes that the scope of addressees shall be limited to the ones who have evidenced potential interest in the subject matter of the communication, and that the latter shall be clearly disclosed within the title of the communication.

141. Such provision is important as it protects consumers from the sending of propaganda not targeted at potentially interested consumers. Commercial messages shall rather be relevant to the potential or effective interests of consumers.

142. Subsection (1) also determines that consumers shall be given the opportunity to decline to receive further communications, and be informed on the source which provided the supplier with the consumer's data.

143. This subsection is important as it helps prevent any future receipt of undesired communications.

144. Subsection (2) qualifies failure to comply with obligations imposed by subsection (1) as an offence, and subjects the supplier to liability on summary conviction to fine for a first conviction which shall be aggravated in the event of subsequent convictions. The amount of the fines was left up to the discretion of beneficiary states.

PART IV – INTERMEDIARIES AND TELECOMMUNICATIONS SERVICES PROVIDERS

Section 25. Liability

145. Section 25 regulates the situations where intermediaries or telecommunications services providers are not liable for transmission of electronic communication.

146. Subsection (1) establishes that where such intermediaries or telecommunications services providers merely provide a conduit for said transmission of electronic communications, they are not liable for relevant contents if they had no knowledge or were not aware of facts that would, to a reasonable person, indicate a likelihood of criminal liability or of liability for a tort in respect of material on the Internet, or do not properly react to notices of unlawful conducts, as long as they: i) do not initiate the transmission; ii) do not select the addressee; iii) perform functions in an automatic, technical manner without selection of the electronic record; and iv) do not modify the electronic record contained in the transmission.

147. Such subsection is important as it exempts intermediaries or telecommunications services providers from liability where they do not know the unlawful actions nor are supposed to know, and are not in control nor are not supposed to be in control, of the unlawful actions.

148. Subsection (2) makes clear that transmission, routing, and access provision exempted from liability under subsection (1) include automatic, intermediate and transient storage of the information transmitted in so far as this takes place: i) for the sole purpose of carrying out the transmission in the information system; ii) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and iii) for a period no longer than is reasonably necessary for the transmission.

149. This subsection is important as it characterizes situations where the intermediaries or telecommunications services providers do not store the information transmitted for purposes other than the fast and impersonal performance of their services.

150. Subsection (3) establishes that intermediaries and telecommunications services providers are not required to monitor any information in order to know or become aware of unlawful actions.

151. This provision is important as intermediaries and telecommunications services providers cannot and shall not implement permanent monitoring or censorship of communications between third parties.

152. Subsection (4) clarifies that nothing in this Section relieves an intermediary or telecommunications services provider from complying with any court order, regulation, or contractual obligation.

153. This subsection is important for stating that it does not purport to replace any specific court, regulatory, or contract determinations, and rather purports to establish general rules on the matter.

154. For instance, situations may exist where some monitoring activity may be performed by intermediaries and telecommunications services providers, such as in the case of "chat rooms" where use of offensive language or the posting of images of children (especially, of child pornography) may possibly (or, to some extent, likely) take place. In those cases, specific laws or court orders may determine that the monitoring is necessary.

Section 26. Procedure for Dealing with Notice of Unlawful Actions

155. Section 26 establishes the procedures to be followed by intermediaries and by telecommunications services providers where they are aware of unlawful actions and have obtained from users of their services information which can not reasonably indicate otherwise.

156. Subsection (1) determines that in such event the intermediaries and telecommunications services providers shall: i) notify appropriate law enforcement authorities, where required by criminal laws in effect; ii) disclose the identity of the person, where authorized by written law; and iii) also where authorized by written law, remove the information or data message from the information processing system under their control, and cease to provide or offer to provide services in respect of that information.

157. Such subsection is important as it requires that notification of authorities, disclosure of identity, and removal of information be performed only where there is legislation supporting such procedures. As such procedures may impair the rights of persons not yet convicted for unlawful actions, it is necessary that they are found to be legitimate under existing legislation.

158. Subsection (2) establishes that failure to disclose knowledge of unlawful content under subsection (1) constitutes an offence. The rationale for such provision is understandable as intermediaries and telecommunications services providers shall not omit information on unlawful actions of which they become aware.

159. However, it shall be noted that subsection (1) subordinates such obligation of notification to compliance with criminal laws in effect. Those laws do not necessarily require or authorize notification for every sort of situation. Therefore, it is key to carefully analyse relevant requirements existing in criminal laws.

Section 27. Offer of Goods and Services in Safe Environment

160. Section 27 requires that suppliers of electronic offering of goods and services ensure a reasonably safe environment, and disclose relevant safety conditions. It also determines that any breach of security which may affect the confidentiality of the consumer's private data shall be immediately informed to the consumer. This Section is important as it protects consumers from dealing with offerings placed on unsafe environments, and compels suppliers to disclose the levels of safety assured.

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
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	LETER	Meredith

Annex 1

Country	Organization	Last Name	First Name
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[10]	J Paul
PRESCOD	Kwesi

[10] 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[11]	J Paul
PRESCOD	Kwesi

[11] 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