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

Electronic Transactions: Assessment Report

HIPCAR

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

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

Electronic Transactions:

Assessment Report

HIPCAR

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

Disclaimer:

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

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

Please consider the environment before printing this report.

Foreword

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

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

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

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

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

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

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

Brahima Sanou
BDT, Director

Acknowledgements

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

In response to both the challenges and the opportunities 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 Ms. Karen Stephen-Dalton and Mr. Kwesi Prescod, who prepared the initial draft documents. The documents were then reviewed, finalized and adopted by broad consensus by the participants at the First Consultation Workshop for HIPCAR's Working Group on ICT Policy and Legislative Framework on Information Society Issues, held in Saint Lucia on 8-March 2010. Based on the assessment report, Model Policy Guidelines and Legislative Texts were developed, reviewed and adopted by broad consensus by the participants at the Second Consultation Workshop held in Barbados on 23-26 August 2010.

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

Without the active involvement of all of these stakeholders, it would have been impossible to produce 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), and Regulatory and Market Environment Division (RME). Comments were also given by Mr. Michael Tetelman. Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

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

Table of Contents

Page

Section I:
Introduction

E-commerce may be simply defined as the use of electronic systems to engage in commercial activities. The transacting of business through electronic means by processing and transmission of digitized information related to persons, products and services (e-commerce) and the use of advanced information and communication technologies to do so makes it very easy for information to be collected, stored, transferred, manipulated and retrieved through electronic means.

Virtually all major business have a website but different types of e-commerce business models exist. These include :

- "Brick and mortar" businesses that have a presence only in the physical world and are without a commercial internet presence and typically use their web-site for passive promotional purposes rather than to engage in online commercial activity).
- "Bricks and clicks" businesses that combine online presence with a physical off line presence, selling from both their web stores and physical stores.
- "Pure-play" or "dot-com" that operate exclusively online.

There are also different classes of e-commerce market including:

- business-to-consumer businesses (B2C) that treats with individual consumers in a retail or service setting;
- business-to-business businesses (B2B) that provide goods or services to other businesses;
- consumer-to-consumer businesses (C2C) that facilitate transactions between individual consumers, for example e-Bay, the online auction site that serves the C2C market and generates revenue from advertising, ancillary services and transactional fees;
- Government-to-business (G2B) and government-to-consumer/citizen (G2C).

E-commerce is a key component in achieving economic growth by ensuring timeliness and accuracy of contractual and financial transactions, allowing for implementation of e-government services, improving the quality of services and reducing the cost of services and increasing transparency and efficiency in the procurement and sale of goods and services.

In order for beneficiary countries to facilitate innovation, enhance competitiveness in e-commerce and to become active players in e-commerce, an environment to enable electronic transactions must be created that can assure equal opportunities, equality and economic development, while affording legal protection for consumers, business and industry in the global environment.

The existing legal impediments that prevent the use 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 must not be restricted to specific technological solutions. The legislation must be flexible and adapted to developments in and be in harmony with international rules and guidelines. Further, the fundamental principles of law should remain uncompromised and the legislation should contribute to establishing confidence in electronic commerce by providing for protection and privacy of consumers.

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 consummated 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 bargains. 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 (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.[2]

The work of many regional international organizations have promoted the development of a legislative frameworks for e-commerce. They include:

- Organization for Economic Co-operation and Development (OECD) which facilitates the creation of international instruments, decisions and recommendations in areas where multilateral agreements may create progress for individual countries in a globalized economy.
- United Nations Commission on International Trade Law (UNCITRAL) – which was established by the United Nations(UN) in 1966 to harmonize the law of international trade – is a core legal body of the United Nations system that works to create accessible, predictable and unified commercial laws.
- 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 Member States. In the particular case, the Directives on Electronic Commerce and Electronic Signatures provide the overarching framework for the trade bloc.

This Report will review and analyse the Electronic Transactions laws either enacted or in latter stages of development by the beneficiary countries of the HIPCAR[3] ICT Legislative Framework Project.

[2] Contribution by Professor Michael Geist, University of Ottawa, Faculty of Law
Director of E-commerce Law, Goodmans LLP, Attachment 4-A guide to E-commerce law.

[3] 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). It is implemented by the ITU in collaboration with the Caribbean Telecommunications union (CTU) and with the involvement of other organizations in the region. (See www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

Section II:
Executive Summary

This Assessment Report has been prepared in accordance with Phase 1 of the Work Plan for the Working Group on ICT Legislative Framework – Information Society Issues under the HIPCAR Project, which makes provision for a critical assessment report of Electronic Commerce (Transactions) existing in a number of States (the "Beneficiary Member States"[4]) in the Caribbean Region. This Assessment Report is for discussion and adoption by the HIPCAR Working Group on ICT Legislative Framework Meeting to be held in Saint Lucia on March 8th – 12th, 2010.

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

Section 3 provides an overview of relevant trends and key issues of the international e-commerce frameworks, which provide the basis for comparison with national laws, and eventual gap analysis.

Section 4 presents a comparative law analysis of a variety of international, regional, and national frameworks which address this particular issue. This review summarizes the intent and approach used in the framework, and also provides some insight into the administrative structure supporting the implementation of the legal framework.

Section 5 identifies key trends and practices in the implementation of Electronic Transactions legal frameworks. This section provides a discussion of the key policy considerations associated with these trends, to provide a conceptual frame of what will be considered in the assessment of existing legislation.

Section 6 provides an overview of the current legislative environments in the Beneficiary Member States vis-à-vis the main issues associated with an effective legal framework for commercial activity in the electronic environment.

Section 7 undertakes an assessment of these legislative frameworks, comparing them against the key principles and trends identified in Section 5. This facilitates the critique and rating of key clauses within the legislative framework.

Section 8 provides a tabular summary of the comparisons undertaken in Section 7, providing a snap shot of the comparative state of current stage of legislative efforts in the Beneficiary Member Stages.

Thereafter is included the bibliography of materials researched as well as the sources of information considered in this Report.

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

Section III:
Overview on Work of International Organizations Relating to e-Commerce (Transactions) Legislation, Trends and Key e-Commerce Issues

3.1 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce

E-commerce is an area of focus for Organisation for Economic Co-operation and Development (OECD) because of its transborder nature and its potential for all countries in the areas of economic growth, trade and improved social conditions. The OECD developed policy in areas ranging from telecommunication infrastructure and services to taxation, consumer protection, network security, privacy and data protection, as well as emerging markets and developing economies. Following its "OECD Action Plan for Electronic Commerce", endorsed by its members in 1998, its work programme focus was to build trust for users and consumers; establish ground rules for the digital marketplace; enhance the information infrastructure for e-commerce; and maximize the benefits of e-commerce. The 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce are designed to help ensure that consumers are no less protected when shopping online than they are when they buy from their local store or order from a catalogue. By setting out the core characteristics of effective consumer protection for online business-to-consumer (B2C) transactions, the guidelines are intended to help eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling online. The guidelines reflect existing legal protection available to consumers in more traditional forms of commerce; encourage private sector initiatives that include participation by consumer representatives; and emphasize the need for co-operation among governments, businesses and consumers. The guidelines feature eight categories of general principles which are:

(i) **Transparent and Effective Protection for Consumers** which is not less than the level of protection afforded in other forms of commerce.

(ii) **Fair Business, Advertising and Marketing Practices** by businesses engaged in electronic commerce.

(iii) **Online Disclosures** – Clear and obvious disclosures

(iv) **Confirmation Process** included in the electronic transaction affording the consumer to express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.

(v) **Secure Payment** mechanisms, including information on the level of security such mechanisms afford.

(vi) **Dispute Resolution** alternatives accessible in a timely manner without undue cost or burden

(vii) **Privacy** in accordance with the recognized privacy principles set out in the *OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data* (1980) to provide appropriate and effective protection for consumers.

(vii) **Education and Awareness** to educate consumers about electronic commerce, to foster informed decision-making by consumers and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

Further, the guidelines prescribe three types of online information disclosures:

(i) information about the business including identification of the business, its legal name, address, contact information and government registration or licence numbers;

(ii) sufficient information about the goods or services to enable consumers to make an informed decision about whether or not to enter into the transaction; and

(iii) information about the transaction including terms, conditions and costs associated with the transaction.

This may include making the information available in multiple languages, an itemization of costs, terms of delivery, as well as details on any limitations or warranties.

3.2 UNICTRAL Model Law on Electronic Commerce

In 1996 United Nations Commission on International Trade Law (UNCITRAL) created a Model Law on Electronic Commerce and a Model Law on Electronic Signatures in 2001 which has been used by many nations to develop their legislative framework for e-commerce. The Model Law on E-Commerce, adopted in 1996 is a basis for evaluation and modernization laws and practices, for transactions involving the use of information and communications technology and for the establishment of relevant legislation where none exists.

It establishes rules and norms that validate and recognize contracts that are formed through electronic means, sets default rules for the formation of contracts and for the governance of electronic contract performance, defines the characteristics of an original document and a valid electronic writing, makes provision for the acceptance of electronic signatures for commercial and legal purposes and supports the admissibility of electronic evidence in courts and quasi- judicial proceedings. [5]

Underlying the UNCITRAL Model Law on E-commerce is the key concept of "electronic equivalence," which is treated with in the specific contexts of:

(i) data equivalence;

(ii) documentary equivalence;

(iii) equivalence or signatures; and consequently

(iv) parity of contracts.

The framework is based on the establishment of a functional equivalent for paper-based concepts such as "writing", "signature" and "original" thereby providing that information or documents will not be denied legal effect or enforceability solely because they are in electronic format.

The default rules provide the conditions that must be met for an electronic communication to constitute a legally effective substitute for a conventional, paper-based communication. The framework is structured to be technology-neutral so that the provisions therein are applicable to transactions initiated through either Internet web interfaces, secure network electronic data interchange, or basic technologies such as fax-based communiqués.

[5] See www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

3.3 European Union Directives

The European Union's framework on electronic Commerce is established by the conjoined effect of two Directives:

1) The E-Signatures Directive, 1999/ 93/ EC; and
2) The E- Commerce Directive, 2000/31/ EC

The Directives are not themselves laws, but provide guidelines to which Member States should structure their domestic legislative systems.

The former Directive, neither contains and overall regulation of electronic signatures, nor addresses entirely the legal recognition of electronic signatures. It is geared to contribute to the harmonization of member states' legislative regimes thereby facilitating the use of electronic signatures. Even in this regard, the framework does not cover all types of authentication/ certification services, being more concerned with the issuers of certificates.

The latter directive develops the key principle of equivalence found in the UNCITRAL model framework, but also goes further to determine some basic rules for the formation of electronic contracts, and thus provide some fundamental structures that will be the foundation of consumer protection in the Union.

Section IV:
E-commerce Legislation Internationally

Introduction

In many countries around the world including Australia, New Zealand , Singapore, South Africa and the Overseas Territories of the United Kingdom (including, Bermuda, the Cayman Islands, and Turks and Caicos Islands) legislation on Electronic Commerce (Transactions) has been enacted based on the UNCTIRAL Model Law on Electronic Commerce 1996. The legislation in some of those countries are outlined and considered in this section of this Report.

4.1 Australia

In order to support and encourage the development of e-commerce, the Australian Government enacted the Commonwealth Electronic Transactions Act in 1999 was a major step towards supporting and encouraging the development of electronic commerce in Australia. The Act is facilitative and it contains rules applying to the interpretation of other legislation. The Act provides that a transaction under a law of the Commonwealth will not be invalid simply because it was conducted by the use of electronic communications. The Act allows any of the following requirements in transactions under Commonwealth law to be fulfilled in electronic form:

- giving information in writing;
- providing a handwritten signature;
- producing a document in material form; and
- recording or retaining information.

The implementation of the Electronic Transactions Act was in two stages.

- Before 1 July 2001 it only applied to those laws of the Commonwealth that were specified in the Electronic Transactions Regulations 2000.
- On or after 1 July 2001 it applied to all laws of the Commonwealth unless they were specifically exempted from application of the Act by the Electronic Transactions Regulations 2000.

The decision to exempt a law from the application of the Act is made by the Attorney General in consultation with other Government Departments based on the intention deliver all services online where possible. The Exemptions are found in Schedule of the Electronic Transactions Regulations.

Each Australian State and Territory has its own Electronics Transactions Act. The Acts are uniform and generally mirror the substantive provisions of the Commonwealth's Electronic Transactions Act. This federal legislation generally reflects the UNCITRAL Model Law on E-Commerce including the default rules relating to, among other things time of receipt and dispatch.

The Uniform Electronic Transactions Act enacted Bill by the Australian States and Territories allows people to deal electronically with many State and Territory departments and agencies in the same way that they are able to deal with many Commonwealth Australian departments and agencies as a result of the enactment of the Commonwealth Electronic Transactions Act. Further, the Uniform Electronic Transactions Acts makes it clear that a person can enter into contracts electronically.

4.2 Canada

Although the UNCITRAL Model Law on e-commerce has not been enacted into federal law in Canada, with one exception all provinces and territories have enacted versions of a Canadian model based on the UNCITRAL Model law on e-commerce.

The Uniform Electronic Commerce Act (UECA), a project of the Uniform Law Conference of Canada (ULCC), obtained official approval in 1999, providing Canada with a legal model for electronic commerce transactions. The subject of more than two years of negotiation, UECA brought much needed certainty to the world of e-commerce. Based largely on the UNCITRAL Model Law, it clarifies issues such as the enforceability and formation of online contracts, the use of electronic agents in the contracting process and at what point an electronic contract is presumed sent and received.

UECA has received widespread approval from Canadian provinces and territories. As of March 2002, all Canadian provinces, with the exception of Quebec, had enacted legislation based on the UECA model. In November 2001, Quebec enacted its own e-commerce legislation that departs from the UECA model.

4.3 European Union (EU)

The European Commission has shaped e-commerce law throughout Europe and around the world since the mid-1990s. Essential directives include:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases;
- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts;
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce");
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

The EU's Electronic Commerce Directive contains several articles that bear direct similarity to principles found in the UNCITRAL Model Law on e-commerce. Although it falls to Member States to implement the directive into national law, the directive does have direct effect in those States that fail to enact e-commerce legislation in a timely manner.

Article 10 of the directive speaks to contracts concluded by electronic means. It provides that Member States shall ensure that their legal system allows contracts to be concluded by electronic means. In particular, Member States are warned not to create obstacles for the use of electronic contracts.

The purpose of the EU Directives on e-signatures is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market. It states that Member States must ensure that electronic signatures meet certain legal and technological standards to satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and that such signatures be admissible as evidence in legal proceedings. It provides that at a minimum, Member States must ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification service provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate being accurate.

The directive provides that Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification service-provider established in a non-EU country are recognized as legally equivalent to certificates issued by a certification-service provider established within the EU provided that the provider meets certain conditions.

Hungary adopted electronic signature legislation in May 2001. The law, which took effect in September 2001, is said to fully compliant with the EU principles. The Hungarian legislation creates two types of electronic signatures – a simple electronic signature and a qualified electronic signature. The legislation appoints the Minister of Education to administer future issues that may arise within the context of the certification of electronic signatures.

The 1997 EU Distance Selling Directive, which was to be implemented by all Member States by May 2000, is particularly important from an e-commerce perspective. The directive mandates that consumers be provided with the following information before the conclusion of any distance contract:

a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;

b) the main characteristics of the goods or services;

c) the price of the goods or services including all taxes;

d) delivery costs, where appropriate;

e) the arrangements for payment, delivery or performance;

f) the existence of a right of withdrawal;

g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;

h) the period for which the offer or the price remains valid; and

i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

Article Six of the directive provides that consumers have a period of at least seven working days in which to withdraw from a distance contract without penalty and without cause. The only charge that may be made to the consumer is the direct cost of returning the goods.

Article Seven of the directive requires the supplier to execute the order within a maximum of 30 days from the day following that on which the consumer forwarded their order to the supplier.

4.4 New Zealand

The Electronic Transactions Act 2002 of New Zealand closely follows both the UNCITRAL Model Law on Electronic Commerce 1996 and the Commonwealth Australian Electronic Transactions Act 1999. The Act is simple and was drafted in consideration of the provisions of the most recent legislation relating to e-commerce in Canada, Australia Ireland and Singapore.

The purpose of the Act is to facilitate the use of electronic technology and the development of electronic commerce by reducing compliance and transaction costs for business and the general public, removing legislative impediments to dealing with government and public authorities electronically; promoting consistency between the law of New Zealand and that major trading partners, particularly Australia and promoting the development of electronic commerce. The Act is merely facilitative and does not make it mandatory for a person to used electronic technology.

The Act achieves its purpose of facilitation by:

a) reducing uncertainty regarding the legal effect of electronic information, and the time and place of dispatch and receipt of electronic communications; and

b) allowing certain paper-based legal requirements, such as a requirement for writing, a signature, or the retention of documents, to be met by using electronic technology that is functionally equivalent to those paper-based legal requirements.

The Act it does not specify or favour particular technologies and applies equally to existing and new technologies and therefore appears to be technology neutral.

The scope of the Act is limited where specific requirement are required with respect to electronic technology and is excluded where the use of electronic technology is in appropriate.

The Act specifies that information is not legally ineffective simply because it is in electronic form or communicated by electronic means, or incorporated by reference in an electronic communication.

The default rules regarding the time and place of dispatch and receipt of electronic communications are set out in the Act. The rules can be overridden by agreement between the parties to an electronic communication and do not apply to the extent that an enactment provides its own rules.

The Act allows certain legal requirements to be met, subject to conditions by using functionally equivalent electronic technology. The legal requirements which can be met by using subject to conditions are as follows:

a) that information be in writing;

b) that information be recorded in writing;

c) that information be given in writing;

d) that information be signed;

e) that a signature or seal be witnessed;

f) that information (whether in paper or electronic form) be retained;

g) that information (whether in paper or electronic form) be provided or produced to a person;

h) that a person be required to provide access to information (whether or electronic form);

i) that a document be compared with an original;

j) the Act specifies the conditions that must be met to achieve functional equivalence. For example, an electronic communication is functionally equivalent to writing only if it is accessible so as to be usable for subsequent reference.

The Act provides that the consent of certain persons must be given as a condition for meeting some legal requirements by using electronic technology.

4.5 Singapore

The Electronic Transactions Act of Singapore was enacted in July 1998 to create a legislative framework for electronic commerce transactions in Singapore that is predictable. The Act specifies the obligations and rights of parties that are transacting business and addresses issues of authentication and non repudiation, the legal aspects of and the use of digital signatures, and electronic contracts. The Act facilitates the use of electronic transactions in the public sector by providing for public authorities to issue licences electronically and to accept filings electronically.

4.6 United States of America

The United States has implemented the UNCITRAL Model law on e-Commerce both at the national and state level but most of the activity initially occurred at the state level, with dozens of states using the Uniform Electronic Transaction Act (UETA), developed by the National Conference of Commissioners on Uniform State Law, as a model. When some state laws began to deviate from UETA, the United States Congress stepped in to create a uniform standard by enacting the Electronic Signatures in Global and National Commerce Act (E-SIGN) in 2000.

There are differences between the UETA and the UNCITRAL Model law on E-commerce. Firstly, a consent provision clarifies that the UETA does not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form. Second, the UETA facilitates the use of electronic signatures for notarization of documents. Thirdly, Section 10 of UETA features rules for where a change or error in an electronic record occurs in a transmission between parties to a transaction.

E-SIGN specifically provides that if there is a modification to UETA, state statutes that incorporate that modification supersede the federal statute. E-SIGN includes strong consumer consent provisions. These provisions require that consumers affirmatively consent before electronic records can be used to provide them with information that, under other law, must be provided or made available to them in writing. Consumers are also granted the right to withdraw their consent. Additionally, E-SIGN contains some fairly expansive provisions related to contracting by electronic agents. The statute provides that a contract may not be denied legal effect solely because its formation or creation involved one or more electronic agents, provided that the action of the electronic agent is "legally attributable" to the person to be bound.

4.7 Other Countries

Many countries from virtually every continent worldwide have used the UNCITRAL Model E-commerce Law as the basis for establishing national e-commerce legislation.

In South America, **Colombia** passed the Electronic Commerce Law 527 in 1999, based on the 1996 UNCITRAL model law. It establishes the validity and admissibility for "data messages," as well as the enforceability of contracts that contain data messages. Additionally, it provides for the validity of digital signatures and delineates standards for the licensure of certification entities and for the issuance of certificates.

In Asia, **Thailand** also passed its own Electronic Commerce Law in 1999. It addresses electronic signatures along with all electronic communications.

In the Americas, **Bermuda** enacted the Electronic Transactions Act in 1999 to address the legal validity and enforceability of electronic signatures and records as well as their admissibility as evidence in any legal proceeding.

In Africa, **Tunisia** enacted the Electronic Exchanges and Electronic Commerce Law in 2000. Although the law addresses the general organization of electronic exchanges it also governs electronic contracts including the validity and execution liability that may arise from that form of contract.

Section V:
Trends and Key e-Commerce Issues

Introduction

The establishment of a regime to facilitate electronically enabled contractual transactions should resist from being overly prescriptive in nature. This is deemed strategic given the continuous state of development and innovation around matters relating to information and communications technologies, and the means and mechanisms which are being developed to leverage their power. This is also in accordance with guidelines by the European Commission which found that existing contract law has been proven appropriately adaptable and robust over centuries of application.

The major common themes which should be included in the establishment of Electronic Transactions frameworks include:

(i) the definition of the scope of the regime, through the clear identification and definition of key electronic concepts including the parties associated with electronic transactions;

(ii) the criteria through which equivalence of electronic documents and their paper equivalents is effected;

(iii) the specific documents for which the regime is inapplicable;

(iv) the definition of the what is necessary for the recognition of contracts formed in an electronic environment;

(v) the definition of electronic signatures and advanced electronic signatures, as opposed to identity identification systems;

(vi) the definition of an administrative framework to provide oversight of service providers of signature-based services;

(vii) the establishment of consumer protection framework to treat with non-traditional questions such as unsolicited communications; and

(viii) the clarification of roles, responsibilities and liabilities of persons who may be used to facilitate the electronic contract, but are not parties to the agreement.

On review of implementation of Electronic Transactions frameworks regionally and worldwide, it has been found that provisions related to:

(i) Privacy and Data Protection; and

(ii) Intellectual Property Protection

have sometimes been included in legislative instruments. While these considerations are required in a comprehensive information society legislative framework, these are not considered in this assessment as:

(i) in the first instance, Privacy and Data Protection issues are considered in another assessment piece undertaken in this HIPCAR Project; and

(ii) in the second instance, considerations established by the World Intellectual Property Organisation (WIPO) are more readily addressed in instruments particularly associated with Copyright and Intellectual Property questions.

This section outlines the major policy considerations associated with the themes identified, elaborating on core considerations which can be used to assess the maturity of the framework.

Section V

5.1 Definition of Key Concepts

Key questions to be addressed with respect to the definition of key concepts are:

- Does the framework identify the legitimate parties in transactions affected?
- Does the framework clearly identify the environments appropriately considered "electronic" for the application of its principles and provisions ?
- Does the framework clearly identify key instruments and systems which are established to be equivalent to an existing paper-based instrument or system?

5.1.1 Critical in the determination of the scope, and applicability of a legislative regime is the definition of key concepts, entities and persons to whom the regime is targeted. This allows the ready identification of the market or markets impacted by the framework, but also allows the ready determination of how the new framework interacts with existing regimes. Electronic Transactions frameworks are meant to be enabling in nature – as such, interface between this and existing regimes are a necessary presumption in the effect of its provisions. Despite this, there are entirely new concepts and persons that will be introduced by this regime. The definition of these concepts and persons, and their roles and responsibilities in assuring the functional equivalence on which the framework is based, is a critical output of an Electronic Transactions framework.

5.1.2 Electronic Transactions frameworks treat primarily with interactions between parties. By the nature of the use of electronic means, these parties need not necessarily be in proximity to each other. Accordingly, in achieving the necessary functional equivalence, Electronic Transactions frameworks must provide satisfactory emulation of concepts associated with determining who are the particular parties involved in the offering and acceptance of the proposal on which the transaction is based. It is recognized however, that persons may establish automated, electronic agents with whom the other party interacts in the formation of the contract. An example of such is the completion of an online purchase between an individual and a vendor's website purchasing function. Accordingly, the definition of originator and addressee should include the persons themselves as well as their electronic agents.

5.1.3 The UNCITRAL Model Framework reinforces that due to the various levels of sophistication of electronically facilitated communications for which its framework is meant to cater, it becomes essential that the scope of applicability of the framework should be explicitly defined. This definition should be broad enough to include interactions enabled via websites or e-mails transmitted over the Internet, as well as via less sophisticated systems such as facsimile transmissions or over the telephone. Each of these systems have their own systems of record generation, document transmission and/ or authenticity verification which must be accommodated in the Electronic Transactions framework.

5.1.4 It must be noted that despite the general principle of the framework providing equivalence, in the context of validating the authenticity of documents which are transmitted in forms that are readily editable, there are particular concerns which must be established in law for the ready, meaningful implementation of the framework. The information society has, as a community, created mechanisms to facilitate the determination of document authenticity, as well as providing such functionality as allowing the electronic signing of entire documents, or information within a document. As such, these terms, including "electronic signatures", "advanced electronic signature", as well as "certificates" which link electronic signatures to individuals and the "certificate service provider" which provides certificates the persons, all of which are considerations specific to the an Electronic Transactions regime, must be clearly detailed.

Section V

5.2 Legal Effect of Electronic Transactions

Key questions to be addressed with respect to the legal effect of electronic transactions are:

- Does the Policy framework explicitly bind the State, thus facilitating e-government services?
- Does the policy framework identify classes of documents for which it will not be applied?
- Does the framework reinforce that the use of electronic means remains voluntary on the part of the users?

5.2.1 Of key interest to regional governments is the possibility of efficiency and cost-effectiveness of the use of electronic mechanisms to stream line government operations. Across the region, governments have all praised the possibilities for "E-Government" to transform the way they provide service to their constituents, and make business with parties more efficient. The interest in this line of endeavour is such that the regional mechanism CARICOM has institutionalized within the *Revised Treaty of Chaguaramas* a centre for the development of governance systems, Caribbean Centre for Development Administration. CARICAD is currently undertaking significant work in developing e-Government frameworks to assist regional development and integration. However, all these initiatives will mean nothing without appropriate enabling frameworks allowing the Government to accept applications, process information and issue notices via electronic means. As current statutory frameworks are particularly paper-centric in the definition of procedures, it is necessary that any electronic transactions framework includes provisions that legally allows government to maximize the use of electronic systems in the conduct of its business. It should be noted that common law dictates by the well established rule of construction[6] that an enactment does not bind or affect the right of the State unless it is expressly stated in the Act. Accordingly, statutory frameworks across the region must include such a statement to ensure applicability of the provisions to the implementation of e-Government.

5.2.2 In accordance with the OECD framework and the UNCITRAL Model law, the frameworks should encourage equivalence of paper and electronic documents. However, Dr. Murray of the London School of Economics and Political Science (LSE) notes that in the EU framework, not long after equivalence is affected in the Directive that certain narrowing of applicability is introduced. He points to four particular types of contract to be excluded from the equivalence principle are introduced:

(i) contracts that create transfers in real estate, not including rental rights – ostensibly done to maintain "the badge of formality" associated with the depth of responsibility of such transactions;

(ii) contracts that by law require the involvement of the courts – which is criticized by some for being vague and unclear to which exactly contracts such exemptions would apply;

(iii) contracts "of suretyship granted" and "collateral securities" – included as a lobby from consumer protection and financial services interests to maintain the same "degree of formality" as mentioned above; and

(iv) contracts governed by "family law or by the law of succession", allowing for the removal of sensitive family documents such as wills, adoption papers, divorce certificates etc. from applicability to the equivalence principle.

There is general acknowledgement that for classes of documents which are not involved in the definition or execution of contracts, or where a single or limited copies of that document is an intrinsic part of the document's value, there should be consideration of exemption from the equivalence provisions of an Electronic Transactions Framework.

[6] pronounced in the case of **Attorney General v. Hancock** [1940] 1 KB 427

5.2.3 The framework must make it clear that nothing in the legislation will require any person to use, provide, or accept information in an electronic form without that person's consent. The aim of the legislation should be to make possible for people to use electronic technology, but not to make it mandatory or compel them to do so and this must be expressed to remove any doubt. As a general rule consent to receive electronic information may be inferred, and need not be expressed in every case. Allowing consent to be inferred not only eliminates the need for unnecessary communication but also reduces the opportunities for after-the-fact bad faith repudiation. However, in the case of Government agencies and public authorities, it may be advisable for consent to expressly stated so that there will be no confusion about when government is "ready to do business" in a particular area electronically. By deferring from the general inference of consent, citizens will not be able to argue that because government places information on a website about licensing requirements for a new business that it should be in a position to take applications for a licence electronically at that time.

5.3 Legal Requirements for the Validity of Electronic Documents

Key questions to be addressed with respect to validity of electronic documents are:

- Does the framework defer from identifying or describing any specific technological solution?
- Does the framework limit the validity of a document solely because of its electronic nature?
- Does the framework provide equivalence between electronic documents and its comparative in writing?
- Does the framework outline conditions to validate the authenticity of an electronic document as an original instrument?
- Does the framework address the admissibility of an electronic document for evidential weight?
- Does the framework require the retention of electronic documents?

5.3.1 As discussed above, electronic commerce can and does include consideration of a wide range of activity, from web–based online purchase agreements to transmittal of documents and information by fax. Accordingly, in applying the dual principles of functional equivalence and technological neutrality there needs to be an explicit statement of the media neutrality associated with the regime. It should be noted that such a provision does not confer any greater importance, security or authenticity to an electronic document. It merely outlines that further tests should be applied to the electronic document or record before its validity in a court can be determined.

5.3.2 Many documents and communications are required by the law of CARIFORUM countries to be "in writing". In some instances provisions require certain communications, and particular types of documents or records to be "in writing", or associated consequences to the absence of writing. The manner in which the information may be recorded and how dealings may occur or be proved may be limited by requirement by law for certain documents or communications to be in "writing" because the use of new technologies would be prohibited despite the electronic communications and records are the functional equivalent of a paper-based records or communications, and may be used at a lower cost and may be more convenient than paper-based records. In many instances the Interpretation Acts of many beneficiary countries impose limits on what would be treated as being in writing, in which case they are too narrow to facilitate the use of all appropriate electronic technologies, and inconsistent with the functional equivalence principle. The UNCITRAL Guide to Enactment notes that writing can be seen as the most basic aspect in the hierarchy of consideration that a document may be subject to for legal validity, which may include signatures, witnessed signatures, etc. Thus it is essential that this basic aspect is appropriately and explicitly addressed so that this first test of validity is met. As above, such a clause confers no special right to electronic documents over their paper equivalent.

5.3.3 On considering the need for a document to be presented as "original" for legal purposes, it is already noted that an Electronic Transactions framework should exclude the applicability to its

equivalence provisions where that requirement is associated with the intrinsic physical document due to its necessary uniqueness as the only (or limited copy). Otherwise, the need for the presentation of "original" documents is to ensure the integrity or unaltered state of the information contained therein. As discussed below, there are technical means established through authentication technologies and certification systems which can readily facilitate this attestation that a document is not altered in the electronic paradigm. Accordingly, in line with the principle of functional equivalence, the framework should provide for electronic document being considered as the original of that document once:

(i) the document can be stored, printed or downloaded by the receiving party; and

(ii) conditions of integrity and reliability of the document are confirmed. Such conditions may include the electronic signing of the document.

5.3.4 The requirement for Evidential Weight recommended by UNCITRAL model frameworks and the EU Directives are achieved through the cumulative effect of concepts articulated before. Where electronic documents can be deemed as original, with associated concerns of integrity and retrievability, the equivalence of "in writing" provisions should provide the document with appropriate weight. In any case, best that practice suggests that such explicit provisions should be included to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value

5.3.5 In accordance with the principles of equivalence, the legal requirement to retain information for various purposes, which is found in the legislation of CARIFORUM countries is met through electronic documents. Such a provision should not require conditions other than existing operational or archival requirements such that if there are retention requirements associated with a paper document, the same must be facilitated by its electronic equivalent to be compliant with the principle of comparative writing. Provisions treating with the validity to stored electronic documents should not prejudice the archival and document preservation programmes which may be underway.

5.4 Formation of Contracts

Key questions to be addressed with respect to the formation of contracts are:

- Does the framework outline how the source of an electronic document is to be attributed?
- Does the framework outline how the time of sending or receipt of an electronic document is established?
- Does the framework outline how the place of residence or work of either party in a transaction is established?
- Does the framework outline requirements treating with errors for a valid electronic contract?
- Does the framework state that the parties of a contract may agree to terms which vary from these provisions ?

5.4.1 In creating the appropriate equivalences between paper and electronic contracts, the framework should model as defaults, key legal constructs that apply in contract law today. However, the legislative framework must make it clear that the default rules do not apply if the parties to a communication agree otherwise, or if an enactment provides otherwise. In treating with the appropriate authorization of either party sending an electronic document in a transaction, the UNCITRAL Model law utilizes a framework that more or less reflects existing law of contracts and agency.

5.4.2 In addressing the question of whether a data message was really sent by the person indicated as being the originator of the message, where in paper-based communication the issue would arise as a question of a forged signature, in an electronically mediated transaction the electronic communication may have been sent by an unauthorized person even where the authentication by code, encryption, electronic signature is accurate. The Model Law on E-commerce deals with this attribution of electronic communications by introducing a presumption that under certain circumstances a data message would be considered as a message of the originator. It qualifies that presumption in case the addressee knew or ought to have known that the data message was not that of the originator.

The principle is that an originator is bound by an electronic communication if the originator has effectively sent that electronic communication. This would include the situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. The question whether the other person has the authority to act on behalf o the originator should be left to the rule in the domestic laws outside of the electronic commerce legislative framework and will not displace the domestic law of agency. To deal with the practical issue of erroneous duplication of electronic communications, the legislative framework should establish a standard of care to be applied by the addressee to distinguish an erroneous duplicate of an electronic communication from a separate electronic communication.

5.4.3 Another key aspect of contract law which may be emulated as appropriate equivalences is the determination of when a document is sent by the originator, or received by the prospective addressee. A number of legal questions turn on the place where a message is sent or received, and the time at which it is sent or received. As a result unnecessary uncertainty may be caused and costs may be incurred in the absence of a clear default rule to determine such a question. It is quite common, for example, for users of electronic commerce to communicate from one State to another without knowing the location of information and communications systems through which the communication is operated. Further the location of information and communications system may change without either of the parties to a communication being aware of the change. Whereas in the paper based environment there are guidelines for same associated with the postmark date, in the context of electronic communication it is suggested in the EU framework that the message be treated as being sent when it leaves the control of the originator, that is, when the originator can no longer prevent the transmission of the document. Similarly, in the context of electronic communication is treated as being received when it enters the computer system that the addressee has designated for receiving messages or that is generally used for messages of that type.

5.4.4 The place of dispatch and receipt of electronic communications is deemed to be the place of business of the person generating the electronic communication and the place of business of the addressee respectively. Where the originator or addressee has more than one place of business, the place with the closer relationship to the underlying transaction is treated as the relevant place of business at which the message is sent or received. Where the originator or addressee has no place of business then the place of dispatch and receipt is deemed to be the ordinary place of residence of the originator or addressee respectively. The legislative provisions proposed for the place of dispatch and receipt is intended to ensure that there is some reasonable and meaningful connection between, for example, the addressee, and what is deemed to be the place of receipt, that can be readily ascertained by the person generating the electronic communication. The provisions are intended to ensure in particular that it is not the location of a server or other computer which determines the place of receipt or dispatch, as this may be quite arbitrary, and is not clear to the other party to the communication. The introduction of such provisions will provide users of electronic technology with a reasonably clear and objective default rule, which will be easy to apply in most cases and which is similar to the provisions contained in the legislation of major trading partners. It additionally will provide for consistency of approach on a regional and international level.

5.4.5 Building on the discussion of 3.3.1, it is expected that a vast amount of electronic transactions will be based on online purchases/ agreements effected between consumers and the electronic agent of a vendor. It can be reasonably expected that from time to time persons may make “key stroke” errors while interacting with the electronic agent. Electronic agents, being only machines, may often not recognize keystroke errors. To prevent such an error, individuals communicating with an electronic agent may be asked to confirm their action by reviewing a summary of the order, or re-entering the information a second time to confirm it. In line with the principle of technology neutrality and the philosophy of encouraging innovation, the framework should not set out any particular form of correction that should be made available since that depends on the situation and will certainly depend on present and future technology. However it is appropriate to provide some form of correction mechanism or protocol. The obligation to establish such a mechanism or protocol should reside with the person offering the contract

or agreement at the risk of bringing the legitimacy of the agreement into question. Once established, if the procedures set out to notify the presence of and correct the error are followed, then the contract made in error is not enforceable. If, however, the party making the error has benefited from the contract by, for example, accepting and using a product, then the contract would be enforceable since that party would be considered to have adopted the terms of the contract even if originally made in error.

5.5 Electronic Signatures

Key questions to be addressed with respect to electronic signatures are:

- Does the framework identify what constitutes an electronic signature?
- Does the framework recognize different classes of electronic signature?
- Does the framework outline how providers of advanced signature services are to be administered?
- Does the framework outline the role, responsibilities and associated liabilities of advanced service providers?

5.5.1 Critical to the implementation of the functional equivalence discussed above, is the ability to validate the authenticity of electronic data as unchanged and a definitive representation of the contract as originally constructed and intended. To this end, electronic signatures are a key instrument in a framework enabling electronic transactions – providing that assurance of data validity. The electronic signature acts as a legal attestation of the authenticity of that document, with equivalence to handwritten signatures (in the case of an individual) or printed names and company stamps (in the case of a firm). It is notable that the European Directive's citation on this issue makes the distinction that references to electronic signature technologies are targeting those systems geared to "data authentication" and do not include under their ambit "entity authentication" technologies such as automatic bank teller PINs, online access to web portals, etc.

5.5.2 It is recognized that as part of its philosophy of technology neutrality, that an electronic signature may take many forms. A signature in such contexts may vary from something as simple words or symbols included in an electronic document to something as complex as public key infrastructure cryptographic codes or attestations. The European Directive validates this approach citing

> "*the rapid technological development of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically.*"

Accordingly, the framework to be developed should also consider applicability of various form of sophistication of electronic signatures.

However, despite this purported intent on technology neutrality, by insisting that an "advanced" electronic signature must meet particular criteria to meet the legal conditions including being:

(i) uniquely linked to the signatory;

(ii) uniquely linked to the signatory;

(iii) capable of identifying the signatory;

(iv) created using means through which the signatory can maintain control; and

(v) linked to the data to which it relates in such a manner that any subsequent change in the data is detectable

some have noted that these obligations describe a particular digital signature technology – public key encryption commonly referred to as "PKI". Notwithstanding same, there have been further developments among international standards agencies specifying advanced electronic signature conformance using other existing standards utilized in the e-mail and document security markets. This development, providing evidence of the power of innovation in a vibrant markets, provides credence for the defined criteria for sophisticated e-signature solutions.

5.5.3 Dr. Murray of LSE notes that online retailing has developed into a particularly important growth component in developed economies. Further, at the heart of the development of online retailing is the ability to enter into and perform online contracts, to which the form of attestation – the electronic signature is extremely relevant. Therefore the way how a government chooses to regulated e-commerce, and by extension of e-signatures, is of central importance to an e-commerce framework – If regulation is too heavy-handed, there is the risk of

"stifling entrepreneurial activity, causing a slow-down in the e-commerce sector."

Alternatively, if the regulation is too weak, there is a

"risk [of] damage[ing] consumer confidence, leading to [a] dangerous downturn",

It is this fine line that must be thread in the establishment of legislative oversight of electronic signatures, and the persons that provide services linking advanced e-signatures to persons – also called "certificates". Certificates themselves have particular obligations to ensure their legal validity, and thereby determination as "qualified" certificates. As qualified certificates will be generated in association with the most sophisticated s-signatures some jurisdiction's frameworks (e.g. Malta) provide additional legal validity to the electronic transactions validated by them. This has had the concomitant impact of defining a niche for such services for the most sensitive of electronic transactions, in terms of content and/ or value.

5.5.4 The establishment of a reliable mechanisms where persons issuing certificates, called "certificate service providers" can enter a domestic market space to provide service is necessary for the development and sustainability of a culture of trust in the use of electronic trading systems by the public. While no frameworks explicitly restricts States from establishing their own CSP's, the most common form through which this service is provided is through private firms. It is notable, that where States establish their own CSP's, there should be conformance to the general principles of open competition, thereby restricting the practice of establishing legal monopolies in this regard.

5.5.5 As global trade expands there should be consideration of the seamless provision of certification services. This concept is given credence due to the ubiquity of the Internet with its ability to allow a provider to service consumers anywhere in the world. This brings to the fore a recurrent theme for policy makers – determining the appropriate regulatory framework to allow market entry to e-service providers that does not restrict innovation, while providing appropriate protections for the consumer including access to speedy dispute resolution. The final approach tends to reflect the regulatory culture of the State – with North American and European States[7] tending to more open access models, while Latin American and Asian approaches tending to various levels of registration and authorization. Whatever the approach for managing market entry, a notable aspect to such regulatory frameworks is that, due to the variety of technologies that can be used, there must be considerable flexibility in how the service is technically provided. The State government's form of administration of this activity must therefore consider the adherence to general practices and procedures, as well as ensure that such service providers provide appropriate risk coverage (financial or otherwise) so as to engender trust and reliability in the provider. The regulatory paradigm should include provisions for the recognition of qualified certificates from CSP's located outside of the State.

5.6 Consumer Protection

Key questions to be addressed with respect to consumer protection are:

- Does the framework provide specific requirements of the vendor in the execution of electronic contracts with consumers?
- Does the framework outline provide for the voidance of electronic contracts?
- Does the framework provide protection of the consumer from unwarranted communications?

[7] No doubt in part to an existing commitment of Member States to the Union.

5.6.1 A fundamental aspect of the European Directive's focus upon the ratification of OECD Guidelines for function equivalence are the inclusion of particular guidelines geared to the providing transparency and consumer protections in on-line transactions. The first element of the physical world transaction that must be emulated in the electronic environment is the amount and type of information that is available to the consumer. When a consumer operates in a face-to-face environment, or even deals with a supplier over the telephone or through the mail, the consumer often has certain information about the supplier – where the supplier is located and how to contact that supplier. In the e-commerce environment, the supplier is often in another – unidentified – country and the consumer may have little knowledge of how to contact or deal with the supplier. To treat with such conditions, the EU Commission noted that:

> *"Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens;"*

Such consideration should be considered in the harmonization of approaches across the Caribbean.

5.6.2 Further, the consumer cannot examine the goods and may have little opportunity to confirm the nature of the services beyond the description available on a website. Assurances of good business practices on the part of the supplier are seen by many as even more important in e-commerce when the consumer may have little recourse or opportunity to seek redress because of lack of information. Indeed, the consumer may not really have the opportunity to exercise a truly informed choice about purchase because of the lack of information. Accordingly, the framework should make provision for the minimum declaration of information by a vendor in an online transaction. As the majority of the risk would otherwise be borne by the customer, penalties for breach of such disclosure obligations should be such that it acts as a disincentive to errant businesses.

5.6.3 In this regard, a primary disincentive is the loss of business. The EU Directive provides a framework where when a consumer has not been provided with the minimum information required, the consumer will have the right to void or rescind the contract, provided that the consumer has not received any material benefit from the contract. However, if the consumer has enjoyed some material gain from the transaction, for example, having received and used the product or the service that was the subject of the contract, then the contract cannot be rescinded. Any supplier in e-commerce who fails to provide the required information, however, runs the risk of having a contract cancelled.

5.6.4 Similarly, while the sending of unsolicited commercial can be seen by some as a valid aspect of a commercial marketing strategy, electronic systems facilitate the multiplication of the scope of such activity. The unfettered sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and service providers alike and may disrupt the smooth functioning of telecommunications networks. Electronic Commerce frameworks, as part of the minimum guidelines of consumer protection, may also propose approaches which form a balance between the right of business to use unsolicited communications as a tool, and the right of the consumer to not be overwhelmed by such correspondence. In this regard, there are two (2) fundamental approaches – either an "opt-in" approach – where the consumer has to provide some form of blanket agreement to receive correspondence before actually receiving the same, or an "opt-out" approach where the consumer is given the opportunity to instruct the sender of the correspondence to desist the activity. While opt-in approaches may be a valid approach to be used when a person enrolls with a service provider or vendor, it is more complex to realistically manage outside of such contexts without seriously impinging upon commerce's ability to use the marketing tool. Therefore, as a default provision, many frameworks have adopted the use of obligatory inclusion of opt-out mechanisms with unsolicited communications.

Section V

5.7 Intermediaries and Telecommunications Providers

Key questions to be addressed with respect to intermediaries and telecommunications providers are:

- Does the framework specify persons that can be identified as intermediaries?
- Does the framework outline responsibilities of intermediaries and telecommunications providers in the facilitation of an electronic contract, or transmittal of an electronic document?
- Does the framework outline limitations to the liabilities of these persons in the instance that there is illegal activity associated with the electronic document or contract?

5.7.1 Telecommunications Service Providers facilitate digital connectivity and transport services to their customers. The networks owned and managed by these providers facilitate the carriage of faxes, e-mails, EDI datagrams or other forms of electronic communiqués. A particular type of Telecommunications Service Provider, the Internet Service Provider (ISP) is specifically identified in many frameworks, due to the nature of the service facilitated – access to the Internet – facilitated the most robust platform for the transmission of digital information between parties. Similarly, an Intermediary refers to parties who provide services which may facilitate electronic communications, these include online e-mail services, web site hosting and online mediation. An ISP may provide intermediary services, or provide subscribers access to independent intermediaries.

5.7.2 For Internet service providers and intermediaries, there is a separation of content from the service of providing carriage for content. Where the common carrier concept of mere carriage or provision of a conduit applies, the intermediary or telecommunications service provider should not be held responsible or liable for content. There is a limitation, however, to how the concept of mere carriage can apply. First, the limitation of liability to the (telecoms or intermediary) service provider is limited to the technical processes associated with operating and giving access to a communication network and/ or service infrastructure. It presumes a mere technical, automatic or passive nature of involvement. However, there are circumstances where that presumption may no longer apply. In such instances, where it can be judged by an objective standard that the service provider became aware of the activity, or that it is determined that a reasonable person in that position would be aware of a likelihood of civil or criminal liability regarding the content being carried or stored, certain obligations should be triggered. These obligations may include, at least, notification to relevant authorities of such action.

Further, where it is determined that the service provider collaborated with one of its recipients, to undertake illegal activity, including being actively involved in the modification of the content, the exemption from liability will not be afforded such service providers.

Section VI:
E-Commerce Legislation in Beneficiary Countries

Introduction

Five HIPCAR beneficiary countries are reported to have e-commerce (transactions) legislation, namely Bahamas, Barbados, Belize, Jamaica and Saint Vincent and the Grenadines. The Electronic Transactions Act of Saint Vincent and the Grenadines although enacted has not been brought into force. With regard to the other Member States, the OECS Member States and Trinidad and Tobago are reported to have Bills at various stages of processing for enactment.

6.1 Barbados

The Barbados Electronic Transactions Act 2001 (the "ETA") is part of a legislative package that also includes the Evidence Act and the Interpretation Act, notably gives legal effect to electronic signatures. The ETA establishes a legal framework for the conduct of e-commerce and processing of electronic transactions. In general, the ETA seeks to improve user confidence by addressing concerns over privacy, security and contract enforcement. The ETA also provides for regulations in respect of encryption, penalties for contravention of disclosure provisions and for records management in relation to the recording of the time and place of dispatch and receipt of electronic records.

6.2 Bahamas

The Electronic Transactions Act, 2003 of Bahamas is targets the treatment the fundamental concerns of functional equivalence of traditional paper-based systems and new electronic mechanisms. In that regard, the Act comprehensively treats with enacting the legal requirements to ensure the validity of electronic documents. The question about electronic signatures and characteristics thereof are deferred to subsidiary regulations. The Act does not treat with ancillary questions such as the administration of service providers of advanced electronic signatures, nor does it treat with concerns of limiting the liability of intermediaries and telecommunications service providers.

6.3 Belize

The main objective of the Belize Electronic Transactions Act 2003 is to eliminate legal barriers to the effective use of electronic communications in legal transactions. The Act is particularly strong in terms of provisions regarding the legal equivalence of electronic documents and default guidelines for online contract formation. While there is recognition of electronic signatures, there is little elaboration in the Act on administrative questions surrounding advanced electronic signatures and the recognition of certificates and Certificate Service Providers.

6.4 Jamaica

The Jamaica Electronic Transactions Act 2006 is aimed at encouraging all citizens of Jamaica to conduct business online. The Act provides the legislative framework necessary to enhance the integrity of and confidence in electronic documents and electronic transactions international and local confidence in the reliability integrity. Drafted in a prescriptive fashion, the Act provides direction on how variations of a number or scenarios shall be treated with in the instance of transactions in an electronic environment. The Act specifically provides consumers with an avenue to lodge their complaints to the Consumer Affairs Commission in accordance the Consumer Protection Act and are afforded a "cooling off" period within which they may cancel certain transactions.

6.5 Saint Vincent and the Grenadines

The Electronic Transaction Act of Saint Vincent and the Grenadines, the primary legislation on e-commerce has not commenced and therefore has no legal force despite being enacted since 2007. This Act sets out new rules to facilitate the use of e-mail and other electronic technology, both in business and in interaction between government and the public. The Act provides for the legal recognition of data messages, records and electronic signatures of. In an attempt to address the security challenges posed by the Internet; the Act requires the "suppliers of cryptography materials" to be registered with the Accreditation Authority established under the Act, who shall be the Minister. Also notable, is the consumer protection provisions of the Act, including consumers' entitlement to a "cooling off" period within which they may cancel certain transactions. The Act also provides the first statutory provisions on Cyber Crimes and introduces statutory criminal offences relating to information systems. These include, among other things unauthorized access to, interception of or interference with data, fraud; and forgery.

6.6 Other Frameworks Being Developed

In many of the Beneficiary Countries that do not have legislation in place relating to electronic commerce draft or model legislation have already been prepared and are at various stages of processing for enactment. In Trinidad and Tobago, for example, the Electronic Transactions Bill has already been introduced in Parliament and in the OECS Member States including Dominica Saint Kitts and Nevis and Saint Lucia the OECS Model Electronic Transactions Bill was approved by the Legal Affairs Committee for enactment in these Sates.

6.6.1 OECS Model Electronic Transactions Bill

The Model Electronic Transactions Bill prepared by the OECS Legislative Drafting Facility is based on the UNCITRAL Model and the Electronic Transactions Act 2002 of New Zealand. While the Model Bill does:

- gives legal effect to electronic information and communications;
- specifies where and when electronic communications are sent and received;
- permits certain legal requirements to be met electronically;
- gives legal effect to electronic signatures;

much of the framing otherwise does not adhere to establishing functional equivalence, developing operational framework to permit the retention of electronic versions of paper-based records and vice versa, while not adequately treating with questions on customer service, intermediaries and the administration of advanced e-signature service providers.

6.6.2 Trinidad and Tobago Electronic Transactions Bill

The Electronic Transactions Bill provides the enabling legal framework for the recognition of electronic documents, records, contracts (with specific exceptions), as well as the rules governing any electronically-enabled business transaction. It establishes the framework by which persons who provide electronic authentication ("certification") services are regulated and facilitates the recognition of electronic signatures. The main highlights of the Bill are as follows:

- It sets out the requirements to be met by an electronic document so that it may be legally recognized as being valid as its paper equivalent.
- It provides the overarching framework for the recognition of electronic signatures.
- It establishes the framework that will guide the regulation of persons who shall provide accredited third party authentication services.

- It treats with the responsibilities of the parties involved in the provision of support services in ecommerce namely, intermediaries and communications service providers.
- Although, it provides that Government and/ or Public Authorities may engage in electronically facilitated transactions in the conduct of business, it does not authorize their acceptance of payment by electronic means.

6.6.3 Grenada Electronic Transactions Bill

The Electronic Transactions Bill provides the enabling legal framework for the recognition of electronic documents, records, contracts (with specific exceptions), as well as the rules governing any electronically-enabled business transaction. It establishes the framework by which persons who provide electronic authentication ("certification") services are regulated and facilitates the recognition of electronic signatures. The Accreditation Authority established by the Act is a government agency that issued accredited signatures in accordance with the prescribed standards. Once accredited, advanced electronic signatures under the Act would carry the State's endorsement and authenticity. The main highlights of the Bill are as follows:

- It sets out the requirements to be met by an electronic document so that it may be legally recognized as being valid as its paper equivalent.
- It provides the overarching framework for the recognition of electronic signatures, including the provision of accredited third party authentication services.
- It establishes the Trade Board as the Certifying Authority to issue accredited certificates
- It treats with the responsibilities of the parties involved in the provision of support services in ecommerce namely, intermediaries and communications service providers.

Section VII:
Assessment of Regional Texts

This Section presents a snapshot of how the key issues listed above are reflected in legal and regulatory texts from the beneficiary countries under the HIPCAR Project (Antigua and Barbuda, The Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago), thereby classifying the situation in the beneficiary countries as related to administration of Electronic Transactions in categories ranging from poor (texts do not make reference at all to key issues) to fair (there is some mention of the issue but it is not detailed or not at an appropriate level, e.g. in some form of consultation document or draft regulation or even in a regulation which is not in line with primary legislation) to good (the texts reflect all elements categorized under a key issue).

Overview of Assessment Ratings:

GOOD: Provisions in law exist which address all major concepts identified by best practice

FAIR: Provisions in law exist which address some of the concepts identified by best practice

POOR: Provisions in law exist which do not adequately address concepts identified in best practice

NONE: There are no provisions in the law which address concepts identified.

LIMITED: There is no law in force which address the issue, however there are such provisions identified in legislation which may have not completed the law-making process (e.g. in legislation laid in the legislature but not passed at the time of report compilation)

* Bills laid before Parliament, not yet passed as statute (as of March 2010).

Section VII

7.1 Legal Mandate

International Best Practices and Regional Trends:

- The framework identifies the legitimate parties in transactions affected
- The framework clearly identifies the environments appropriately considered "electronic" for the application of its principles and provisions
- The framework clearly identifies key instruments and systems which are established to be equivalent to an existing paper-based instrument or system

Antigua and Barbuda – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Bill 2006]
****

"addressee", in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record

"certificate" means an electronic record which purports to ascertain the identity of a person or entity who at the time of creation of that record controls a particular signature device;

"electronic" means relating to technology having electrical, magnetic, optical, electromagnetic, or similar capabilities, whether digital, analogue or otherwise

"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;

"electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

"information" includes electronic records, data, text, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for generating, sending, receiving, storing or otherwise processing information;

"information security service" and "information security procedure" includes a service or procedure which is provided to an originator, intermediary, or recipient of an electronic record, and which is designed to –

(a) secure that the record can be accessed, or can be put into an intelligible form, only by certain persons; or
(b) secure that –
    (i) the authenticity;
    (ii) the time of processing; or
    (iii) the integrity, of such a record, is capable of being ascertained;

"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 –

(i) a person who sends an electronic record on the instructions of another; or

(ii) a person acting as an intermediary with respect to that electronic record;

"record" means information that is inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form;

The Bahamas – GOOD – Definitions provided of identified key concepts.

[Electronic Communications and Transactions Act 2003]

****

"addressee" in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication

"electronic" means relating to technology and having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities

"electronic agent" means a program, or other electronic or automated means that is used independently to initiate or respond to electronic communications or performances in whole or in part without review by an individual;

"electronic signature" means any letters, characters, numbers, sound, process or symbols in electronic form attached to, or logically associated with information that is used by a signatory to indicate his intention to be bound by the content of that information;

"information" includes data, text, documents, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for creating, generating, sending, receiving, recording, storing, displaying, or otherwise processing information;

"originator" in relation to an electronic communication, means a person by whom, or on whose behalf, the electronic communication purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that electronic communication

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

"signed" or "signature" includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic methods;

Barbados – GOOD – Definitions provided of identified key concepts.

[Electronic Transactions Act, CAP. 308B]

****

"addressee", in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

"accredited certificate" means an electronic record that

(i) associates a signature verification device to a person,

(ii) confirms the identity of that person,

(iii) is issued by an authorized certification service provider, and

Section VII

(iv) meets the relevant criteria;

"authorized certification service provider" means a certification service provider authorized under section 18(2) to provide accredited certificates;

"certification service provider" means a person who issues identity certificates for the purposes of electronic signatures or provides other services to the public related to electronic signatures;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information-processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information;

"originator", in relation to an electronic record, means a person by whom, or on whose behalf, the electronic record purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that electronic record;

"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;

"signature creation device" means unique data, including codes or private cryptographic keys, or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

"signature verification device" means unique data, including codes or public cryptographic keys, or a uniquely configured physical device which is used in verifying an electronic signature;

Belize – FAIR – Definitions only associated with concepts associated with the electronic environment. Does not include definitions for, or terms which are the equivalence of "certificates", "certificate service providers".

[Electronic Transactions Act, 2003 Chap 290:01]

****

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

"electronic signature" means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with a document;

"information system" means a system for generating, sending, receiving, storing or otherwise processing electronic communications;

Dominica – NONE

Dominican Republic – GOOD

(INFORMAL TRANSLATION)

(b) digital document: the information encoded in the form Digital on a logical or physical support, which use methods of photolithography, electronic, optical or similar that they are representing acts, facts or legally relevant data;

Section VII

(c) data messages: the information generated, sent, received, stored or communicated by electronic means, optical or similar, as they could be, among others, the electronic interchange of data (EDI), mail electronic, telegram, telex or telefax;

(d) electronic data interchange (EDI): transmission electronic information from one computer to another, When the information is structured in accordance with any technical standard agreed for that purpose;

(e) initiator: any person who, to the tenor of a message from data, you have acted on their own or in whose name has been acted, to send or to generate the message before being filed, if this is the case, but that has not done so to title of an intermediary with respect to this message;

(f) recipient: the person designated by the originator for receive the message, but that is not acting in their capacity of an intermediary with respect to this message;

(g) intermediary: any person who, in connection with a specified message data, acting on behalf of another, send, receive or archive the message or pay someone else service on him;

(h) information system: means that everything used to generate, send, receive, file system or processing of any other digital documents or data messages;

(i) digital signature: shall be understood as a numeric value to be adheres to a data message and which, using a known mathematical procedure associated with the key of the initiator and the text of the message, to determine which This value has been obtained exclusively with the key of the initiator and the text of the message, and that the initial message has not been modified after made the transmission;

(j) Cryptography: is the branch of applied mathematics and the computer science deals with the transformation of digital documents and data messages from your original representation to an unintelligible representation and indecipherable that it protects and preserves the content and form, and the recovery of the document or message of original data from this;

(k) certification entity: is the institution or legal person, authorized in accordance with the present law, is empowered to issue certificates in relation with the digital signatures of the persons, offer or facilitate registration and time stamping services the transmission and reception of data messages, as well comply with communications-related functions based on digital signatures;

(l) certificate: is the digital document issued and signed digitally by an entity for certification that It uniquely identifies a Subscriber during the period validity of the certificate, and is in testing the Subscriber is source or originator of the content of a digital document or data message Enter your associate certificate;

(m) repository: is an information system for the storage and retrieval of certificates or other information relevant to the issuance and validation of the same;

Grenada* – LIMITED (FAIR) – Workable definitions, however those associated with signatures are technology specific and possibly limiting in nature. Proposals in alignment with those used by Jamaica.

[Electronic Transactions Bill, 2008]

“addressee” means a person who the originator of an electronic document intends to receive the document, but does not include a person acting as an intermediary with respect to that document;

Section VII

"accredited certificate" means an electronic record that:

(a) associates a signature verification device to a person;
(b) confirms the identity of that person;
(c) is issued by an authorized certification service provider; and
(d) meets the relevant criteria;

"authorized certification provider" means a certification service provider authorized under section [18(2)] to provide accredited certificates;

"automated communications device" means a computer program or an electronic or other automated device used to initiate or respond to electronic communications in whole or in part, without review or action by a n individual;

"certificate" means any record that:

(a) identifies the entity that issues it;
(b) names or otherwise identifies the signatory or a device (including an automated communications device) under the control of the signatory;
(c) specifies its operational period;
(d) is digitally signed by the entity that issues it;
(e) contains a public key that corresponds to a private key under the control of the originator of the electronic document to which the certificate relates; and
(f) specifies any other matter required to be specified by regulations made pursuant to section 47

"certification service provider" means a person who issues certificates for the purposes of electronic signatures or provides to the public other services related to electronic signatures;

"Certifying Authority" means the Certifying Authority established under section 42;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities and references to carrying out any act "electronically" shall be similarly construed;

"electronic document" means information created, , generated, communicated, stored, displayed or processed by electronic means[but not limited to electronic data interchange, electronic mail, telegram, telex or telecopy;

"electronic signature" means information that:

(a) is contained in, attached to or logically associated with, an electronic document; and
(b) is used by a signatory to indicate his adoption of the content of that document,

but does not include any signature produced by a facsimile machine or an electronic scanning device;

"encrypted signature" means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for creating, generating,[producing], sending, receiving, recording, storing, displaying or otherwise processing information;

"originator", in relation to an electronic document, means a person by whom, or on whose behalf, the document purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that document

Section VII

"signature" includes –
(a) any symbol executed or adopted; or
(b) any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;

"signature creation device" means unique data, including codes or private cryptographic keys , or a uniquely configured physical device which is used in verifying an electronic signature;

"signature verification device" means:
(a) unique data, including codes or public cryptographic keys; or
(b) a uniquely configured physical device, which is used in verifying an electronic signature;

Guyana – NONE

Haiti – NONE

Jamaica – GOOD (FAIR) – Workable definitions, however those associated with encrypted signatures seem to identify a particular technology and therefore is possibly limiting in application.
[Electronic Transactions Act, 2006]
****

"addressee" means a person who the originator of an electronic document intends to receive the document, but does not include a person acting as an intermediary with respect to that document;

"automated communications device" means a computer program or an electronic or other automated device used to initiate or respond to electronic communications in whole or in part, without review or action by a n individual;

"certificate" means any record that:
(a) identifies the entity that issues it;
(b) names or otherwise identifies the signatory or a device (including an automated communications device) under the control of the signatory;
(c) specifies its operational period;
(d) is digitally signed by the entity that issues it;

(e) contains a public key that corresponds to a private key under the control of the originator of the electronic document to which the certificate relates; and
(f) specifies any other matter required to be specified by regulations made pursuant to section 37

"certification service provider" means a person who issues certificates for the purposes of electronic signatures or provides to the public other services related to electronic signatures;

"Certifying Authority" means the Certifying Authority established under section 33;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities and references to carrying out any act "electronically" shall be similarly construed;

"electronic document" means information created, , generated, communicated, stored, displayed or processed by electronic means;

"electronic signature" means information that:
(a) is contained in, attached to or logically associated with, an electronic document; and
(b) is used by a signatory to indicate his adoption of the content of that document,
but does not include any signature produced by a facsimile machine or an electronic scanning device;

Section VII

"encrypted signature" means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device;

"encrypted signature creation device" means unique data, including codes or private cryptographic keys , or a uniquely configured physical device which is used in verifying an encrypted signature;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"originator", in relation to an electronic document, means a person by whom, or on whose behalf, the document purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that document

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (FAIR) – Limited consideration within the definitions of persons required to provide certification services in the market.
[Electronic Transactions Bill, 2007]
****

"electronic signature" means information that:
(a) is contained in, attached to or logically associated with, an electronic document; and
(b) is used by a signatory to indicate his adoption of the content of that document,

but does not include any signature produced by a facsimile machine or an electronic scanning device;

"encrypted signature" means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device;

"encrypted signature creation device" means unique data, including codes or private cryptographic keys , or a uniquely configured physical device which is used in verifying an encrypted signature;

Saint Vincent and the Grenadines – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2007]
****

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

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

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

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring -
(a) that the data can be accessed only by relevant persons;
(b) the authenticity of the data;
(c) the integrity of the data;
(d) that the source of the data can be correctly ascertained;

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

Section VII

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

(a) that the data or data message can be accessed or can be put into an intelligible form only by certain persons;
(b) that the authenticity or integrity of the data or data message is capable of being ascertained;
(c) the integrity of the data or data message; or
(d) that the source of the data or data message can be correctly ascertained;

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

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

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

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

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

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

Suriname – NONE

Trinidad and Tobago* – LIMITED (GOOD) – Definitions provided of identified key concepts.
[Electronic Transactions Bill, 2009]
****

"addressee" in relation to an electronic data message means a person who is intended by the originator to receive the electronic data message but does not include a person acting as an intermediary with respect to that electronic data message;

"certificate" means an electronic attestation that links certain signature verification information to the signatory and confirms his or its identity;

"data" means the content including but not limited to the text, images or sound which make up a data message;

"data message" means any document, correspondence, memorandum, book, plans, map, drawing, diagram, pictorial or graphic work, photograph, audio or video recording, machine-readable

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

"electronic agent" means a program configured and enabled by a person that is used to initiate or respond to electronic data messages or performance in whole or in part without review by a person at the time of the initiation or response;

Section VII

"electronic signature" means information in electronic form affixed to, or logically associated with an electronic data message which may be used to–
(a) identify the signatory in relation to that electronic data message; or
(b) indicate the signatory's approval of the information contained within that electronic data message;

"information" includes data, codes, computer programs, software and databases;

"information system" means a device or combination of devices including input and output devices capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that perform logic, arithmetic, data storage and retrieval, communication control and other functions but does not include a calculator;

"originator" in relation to an electronic data message means a person by whom or on whose behalf the electronic data message purports to have been sent or generated prior to storage, but does not include a person acting as an intermediary with respect to that electronic data message;

"record" means recorded information collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide evidence or proof of that activity or transaction;

International Best Practices and Regional Trends

1. OECS Model Law

"information system" means a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications;

"electronic" includes electrical, digital, magnetic, optical, electromagnetic, biometric and photonic;

"electronic communication" means a communication by electronic means;

"information" includes information, whether in its original form or otherwise, that is in the form of a document, a signature, a seal, data, text, images, sound or speech;

"information system" means a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications;

2. UNCITRAL Model Law e-Commerce

****

Article 2. Definitions

For the purposes of this Law:

- (a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;
- (b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;
- (c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

- (d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;
- (e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;
- (f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

3. UNCITRAL Model Law e-Signatures

Article 2 Definitions

For the purposes of this Law:

(*a*) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

4. EU Directive 1999/ 93/ EC

****

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

Section VII

12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Section VII

7.2 Legal Effect of Electronic Transactions

International Best Practices and Regional Trends

- The framework explicitly binds the State, thus facilitating e-government services
- The policy framework identifies instances or classes of document for which it will not be applied
- The framework reinforces that the use of electronic means remains voluntary on the part of the users

Antigua and Barbuda – LIMITED (GOOD/FAIR) – Comprehensive language utilized to effect policy best practice. However there is no prescription reinforcing that the Act does not oblige persons to use Electronic means to conduct transactions, or the question inferred consent.

[Electronic Transactions Bill 2006]

****

3. (1) Nothing in this Act shall apply to –
   (a) the grant of a Power-of-Attorney;
   (b) a trust ;
   (c) a will ;
   (d) any contract for the sale or conveyance of immovable property or any interest in such property;
   (e) the swearing of affidavits or statutory declarations before a Commissioner of oaths and notary public or
   (f) the authentication of documents if specifically required to be done by law after a physical inspection and comparison with an original of such document where the original does not exist in electronic data format and has subsequently not be reduced into an electronic data format which integrity is not challenged by the originator of such document.

(2) The Minister may provide by regulations subject to affirmative resolution that this Act, or such of its provisions as may be specified in the regulations-
   (a) shall not apply to any class of transactions, persons, matters or things; or
   (b) shall apply to any class of transactions, persons, matters or things specified under paragraphs (a) to (g).

13. (1) This Act binds the State.

(2) Notwithstanding subsection (1), nothing in this Act shall require a ministry or public body to process an electronic record, but either the Minister or the appropriate minister or official member may, by notice published in the Gazette, indicate that a ministry or public body will process electronic records relating to such matters as may be specified in the notice.

(3) Until a notice under subsection (2) has been published, no person dealing with such ministry or public body shall be entitled, by means of an electronic record, to satisfy a requirement to process a record.

(4) The State, the Minister, or any employee of the State shall not be liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.

Section VII

The Bahamas – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Communications and Transactions Act 2003]
****

3.(1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act obliges any public body to generate, send, receive, store or otherwise process any record by electronic means, but the Minister may, by notice published in the Gazette, indicate that a public body may receive and process electronic communications relating to such matters as may be specified in the notice.

4. Part II shall not apply to any rule of law requiring writing or signatures for the following -
(a) the creation, execution, amendment, variation or revocation of -
(i) a will or testamentary instrument; or
(ii) a trust;
(b) the conveyance of real property or the transfer of any interest in real property;
(c) court orders or notices, or official court documents required to be executed in connection with court proceedings;
(d) enduring powers of attorney to the extent that they concern the financial affairs or personal care of an individual;
(e) all other deeds and documents described in section 3 of the Registration of Records Act, not otherwise expressly provided for under this subsection.

5.(1) Nothing in this Act shall -
(a) require any person to use or accept electronic communications, electronic signatures, or electronic contracts; or
(b) prohibit any person engaging in a transaction through the use of electronic means from -
(i) varying by agreement any provision relating to legal recognition and functional equivalency of electronic communications, signatures, and contracts specified in Part II; or.
(ii) establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

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

Barbados – GOOD (FAIR) – Comprehensive language utilized to effect policy best practice. However there is no prescription reinforcing that the Act does not oblige persons to use Electronic means to conduct transactions, or address the question of inferred consent.
[Electronic Transactions Act, CAP. 308B]

3. (1) Parts II and III do not apply to any rule of law requiring writing or signatures for the following matters:
(a) the making, execution or revocation of a will or testamentary instrument;
(b) the conveyance of real property or the transfer of any interest in real property; or
(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts.

(2) Nothing in this Act requires a person who uses, provides or accepts information or a document, to use, provide or accept it in an electronic form without the consent of that person.

(3) Consent for the purpose of subsection (2) may be inferred from a person's conduct if there exists a reasonable assurance that the consent is genuine and that it applies to the information or document.

28. (1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act requires any Government Department or Government Agency to generate, send, receive, store or otherwise process any record by electronic means; but the Minister may, by notice published in the *Official Gazette*, indicate that a Government Department will receive and process electronic records relating to such matters as may be specified in that notice.

Belize – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2003 Chap 290:01]
****

5. This Act binds the Crown.

14. (1) If a public body has power to create, collect, receive, store, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the power to do so electronically.

(2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

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

(4) Where a public body consents to receive any information in electronic form, it may specify:
- (a) the manner and format in which the information shall be communicated to it;
- (b) the type or method of electronic signature required, if any;
- (c) control processes and procedures to ensure integrity, security and confidentiality of the information;
- (d) any other attributes for the information that are currently specified for corresponding information on paper.

(5) The requirements of subsections 7(1) and (3) and section 8 also apply to information described in subsection (4).

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

…

15. This Act does not apply to:
- (a) the creation or transfer of interests in real property;
- (b) negotiable instruments;
- (c) documents of title;
- (d) wills and trusts created by will; and
- (e) any class of documents, transactions or rules of law excluded by regulation under this Act.

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

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

Section VII

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

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

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

Dominica – NONE

Dominican Republic – NONE

Grenada* – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Bill, 2008]

3. This Act does not apply to the transactions specified in the First Schedule to the extent specified in that Schedule.

6. (1) Except as provided in Part IV nothing in this Act shall be construed as imposing an obligation on any person to create, give, store or receive any information electronically.

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

(3) The fact as to whether or not a party has agreed to conduct a transaction electronically shall be determined
(a) if the party is the Government, by express stipulation by the Government;
(b) in the case of any other party, by the context and surrounding circumstances , including the party's conduct.

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

(5) Except as otherwise provided in this Act, any provision of Part II or Part III may be varied by agreement between the parties to a transaction conducted electronically.

47. This Act binds the Crown.

First Schedule
1. the making, execution, alteration or revocation of a Will or testamentary instrument;
2. the conveyance of real property or the transfer of any interest in real property;
3. negotiable instruments;
4. the creation, performance or enforcement of an indenture, declaration of trust or power of attorney , [other than constructive and resulting trusts.]
5. Any procedure governed by the [Civil Procedure Rules] or by rules of court made pursuant to any law.

Guyana – NONE

Haiti – NONE

Section VII

Jamaica – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2006]
****

4. The provisions of the Act shall not apply to the transactions set out in the first Schedule, to the extent specified in the First Schedule.

5. (1) Except as provided in Part IV, nothing in this Act shall be construed as imposing an obligation on any person to create, give, store or receive any information electronically.

(2) this Act applies to any transaction between parties each of whom has agreed to conduct the transaction electronically

(3) the fact as to whether or not a party agrees to conduct a transaction electronically shall be determined –
(a) where the party is the Government, by express stipulation of the Government;
(b) in the case of any other party, by the context and surrounding circumstances including the party's conduct

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

(5) Except as otherwise provided hereunder, as between the parties to a transaction conducted electronically, any provision of Part II or Part III may be varied by agreement
…
36. This Act binds the Crown.

First Schedule
1. The making, execution, alteration or revocation of a Will or other testamentary instrument
2. The conveyance or transfer of real property or any interest in real property.
3. The creation, variation, performance or enforcement of any –
(a) trust; or
(a) power of attorney
4. Any procedure governed by the Civil Procedures Rules, 2002, or by the rule of court made pursuant to any law

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (GOOD)
[Electronic Transactions Act, 2007]
****
3. This Act does not apply to:
(a) the creation or transfer of interests in real property;
(b) negotiable instruments;
(c) documents of title;
(d) wills
(e) trusts created by will; and
(f) any class of documents, transactions or rules of law excluded by regulation under this Act.

This Act binds the State
…

14. (1) This Pat does not authorize a person to use, provide, or accept information in an electronic form without that person's consent.

Section VII

(2) For the purposes of this Part and subject to subsection (3).-

(a) a person may consent to use, provide, or accept information in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored, or displayed;

(b) consent may be inferred from a person's conduct.

(3) The consent of a public body to accept information in electronic firm may not be inferred from its conduct but must be expressed by communication accessible to the public or to those most likely to communicate with it for particular purposes.

(4) This Part does not authorize a public body to require any person to give, provide or accept information in electronic form without consent.

Saint Vincent and the Grenadines – GOOD – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Act, 2007]

****

3. This Act shall bind the Crown.

…

13. This Act does not apply to:

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

(b) negotiable instruments;

(c) documents of title;

(d) wills and trusts created by wills;

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

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

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

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

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

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

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

Suriname – NONE

Section VII

Trinidad and Tobago* – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Bill, 2009]
****

3. This Act binds the State.

4. (1) Parts II, III and IV of this Act shall not apply to any written law requiring writing, signatures or original documents for–
(a) the making, execution or revocation of a will or testamentary instrument;
(b) the conveyance of real or personal property or the transfer of any interest in real or personal property;
(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney;
(d) the production of documents relating to immigration, citizenship or passport matters; or
(e) any other matters that may be determined by the Minister by Order.

(2) Notwithstanding subsection (1), the Minister may by Order make this Act applicable to any of the legal requirements set out in subsection (1).

(3) An Order made under subsection (2) shall be subject to affirmative resolution of Parliament.

(4) Unless otherwise provided by any other written law, this Act shall not apply to electronic funds transfers.

5. This Act does not require a person who uses, provides, accepts or retains a document record or information, to use, provide, accept or retain it in an electronic form.
…

7. Notwithstanding Parts II, III and IV, this Act does not limit the operation of any written law that expressly authorizes, prohibits or regulates the use of information, data messages, records, payments or signatures in electronic form or requires that information, a data message, a record or a payment be posted or displayed in a specific manner.
...

54. In the absence of a specific legal provision that electronic means may not be used or that electronic means shall be used in a specific way, the Government of Trinidad and Tobago and other public authorities may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with records or information.

55. Subject to section 54, the authority under any law or regulation to issue, prescribe or in any other manner establish a form or to establish the manner of filing a document or submitting information, includes the authority to issue, prescribe or establish an electronic form or to establish an electronic manner of filing the document or submitting the information.

International Best Practice and Regional Trends

1. OECS Model Law
****

Application
3. This Act binds the Crown

Section VII

Consent to Use of Electronic Technology

12 (1) Nothing in this Part requires a person to use, provide, or accept information in an electronic form without that person's consent.

(2) For the purposes of this Part,-

(a) a person may consent to use, provide, or accept information in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored, or displayed;

(b) consent may be inferred from a person's conduct

2. EU Directive 2000/ 32/ EC

****

GENERAL PROVISIONS

Article 1

Objective and Scope

1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.

5. This Directive shall not apply to:

(a the field of taxation;

(b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;

(c) questions relating to agreements or practices governed by cartel law;

(d the following activities of information society services:

– the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,

– the representation of a client and defence of his interests before the courts,

– gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Section VII

7.3 Legal Requirement for the Validity of Electronic Documents

International Best Practices and Regional Trends

- The framework limits the discrimination against a document solely because of its electronic nature
- The framework defers from identifying or describing any specific technological solution
- The framework provides equivalence between electronic documents and its comparative in writing
- The framework addresses the admissibility of an electronic document for evidential weight
- The framework requires the retention of electronic documents
- The framework outlines conditions to validate the authenticity of an electronic document as an original instrument

Antigua and Barbuda – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Bill 2006]

****

5. Information shall not be denied legal effect or validity solely on the ground that it is -
   (a) in the form of an electronic record; or
   (b) referred to but not contained in an electronic record.

6. (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract to be in writing, or is described in any statutory provision or contract as being written, that requirement, permission or description may be met by information in the form of an electronic record.

(2) Subsection (1) shall apply if the requirement for the document, record or information to be in writing is in the form of an obligation or if the statutory provision or rule of law or contract provides consequences if it is not in writing.

7. (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract to be delivered or sent to a person, that requirement or permission may be met by delivery of it in the form of an electronic record if –
   (a) the format of the electronic record and the means of delivery is acceptable to the parties; and
   (b) where the originator of the electronic record states that the receipt of the electronic record is to be acknowledged, the addressee has knowingly acknowledged the receipt.

(2) Subsection (1) applies whether or not the requirement for delivery or sending is in the form of an obligation or whether or not the statutory provision, rule of law, contract provides consequences for the document, record or information not being delivered or sent.

8. (1) (a) Where a statutory provision, rule of law, or contract requires conclusive evidence of the original form of a document, record or information to be presented or retained that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.
   (b) Paragraph (a) shall apply if the requirement for the presentation or retention of evidence of the original form of document, record or information is in the form of an obligation or if the statutory provision, rule of law, contract provides consequences if conclusive evidence of the original form of document, record or information is not provided.

Section VII

(2) (a) Where a statutory provision, rule of law, or contract requires a document, record or information to be presented or retained in its original form and such document, record or information was first generated in its final form as an electronic record, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.

(b) Paragraph (a) shall apply if the requirement to present or retain the document, record or information in its original form is in the form of an obligation or if the statutory provision, rule of law or contract provides consequences if the original form of the document, record or information is not presented or retained.

(3) For the purposes of subsections (1) and (2) the document, record or information is accurately represented where it has remained complete and unaltered from the time it was first generated in its final form, whether as an electronic record or on any other medium, apart from the application of an information security procedure, or apart from –

(a) the addition of an endorsement; or

(b an immaterial change, which arises in the normal course of communication, translation, conversion, storage or display.

9. (1) Where documents, records or information are required by any statutory provision or rule of law or by contract [or by deed] to be retained, that requirement is met by retaining them in the form of electronic records if –

(a) the information contained in the electronic record is accessible and capable of retention for subsequent reference;

(b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the document, record or information when it was generated, sent or received;

(c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent and received is retained; and

(d) appropriate steps are taken to ensure the security of such electronic records in compliance with guidelines which may be prescribed in regulations made by the Minister.

(2) An obligation to retain documents, records or information, in accordance with subsection (1) does not extend to information, the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of another person, if the conditions set out in subsection (1)(a), (b), (c) and (d) are met.

10. Where documents, records or information are required by any statutory provision or rule of law or by contract or by deed to be made available for inspection, that requirement shall be met by making such documents, records or information available for inspection in perceivable form as an electronic record.

11. In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied solely on the grounds that it is an electronic record or an electronic signature.

Section VII

The Bahamas – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Communications and Transactions Act 2003]
****

7. An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is -
(a) in electronic form; or
(b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication.

8.(1) Where information is required by law either to be in writing or is described as being written, such requirement or description is met by an electronic communication if the information contained in the electronic communication is accessible to, and is capable of retention by, the intended recipient.

(2) Subsection (1) shall apply whether the requirement for the information to be in writing is in the form of an obligation or the law provides consequences if it is not in writing.

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

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

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

10.(1) Where information is required by law to be presented or retained in its original form, that requirement is met by an electronic communication if –
(a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its / final form as an electronic communication or otherwise; and
(b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

(2) Subsection (1) shall apply whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of subsection (1)(a) -
(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
(b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances

11.(1) Where certain documents, records or information are required by law to be retained, that requirement is met by retaining electronic communications if the following conditions are satisfied -
(a) the information contained in the electronic communication is accessible so as to be usable for subsequent reference;

(b) the electronic communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
(c) any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received is retained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) shall not extend to any information the sole purpose of which is to enable the message to be sent or received.

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

(4) Nothing in this section shall preclude any public body from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of such public body.

12.(1) In any legal proceedings, nothing in the' rules of evidence shall apply so as to deny the admissibility of an electronic communication in evidence solely on the ground that it is in electronic form.

(2) Information in the form of an electronic communication will be given due evidential weight and in assessing the evidential weight of an electronic communication, regard shall be had to -
(a) the reliability of the manner in which the electronic communication was generated, stored or transmitted;
(b) the reliability of the manner in which the integrity of the information was maintained;
(c) the manner in which the originator was identified; and
(d) any other relevant factor.

Barbados – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, CAP. 308B]
****

5. Information shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that
(a) it is in the form of an electronic record; or
(b) it is not contained in the electronic record purporting to give rise to legal effect, but is referred to in that electronic record.

6. (1) Where the law requires information to be in writing or is described in any statutory provision as being written, that requirement or description is met by an electronic record if the information contained in the electronic record is accessible and is capable of retention for subsequent reference.

(2) Subsection (1) applies whether the requirement for the information to be in writing is in the form of an obligation or the law provides consequences if it is not in writing.

7. (1) Where the law requires information to be delivered, dispatched, given or sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic record if the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee has acknowledged its receipt.

(2) Subsection (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

Section VII

8. (1) Where the law requires the signature of a person, that requirement is met in relation to an electronic record if
   (a) a method is used to identify that person and to indicate that person's approval of the information in the electronic record; and
   (b) that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) An electronic record that meets the requirements of paragraphs *(a)* and *(b)* of subsection (1) shall not be denied legal effect, validity and enforceability solely on the ground that it is an electronic signature.

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

9. (1) Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic record
   (a) if there exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form as an electronic record or otherwise; and
   (b) where it is required that information be presented, if that information is capable of being accurately presented to the person to whom it is to be presented.

(2) Subsection (1) applies whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of paragraph *(a)* of subsection (1)
   (a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
   (b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

10. (1) Where the law requires that certain documents, records or information are to be retained, that requirement is met by retaining electronic records if the following conditions are satisfied:
   (a) the information contained in the electronic record is accessible and is capable of retention for subsequent reference;
   (b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
   (c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received is retained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) does not extend to any information the sole purpose of which is to enable the electronic record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out in paragraphs *(a), (b)* and *(c)* of subsection (1) are met.

11. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic record in evidence solely on the ground that it is an electronic record.

(2) Information in the form of an electronic record shall be given due evidential weight and in assessing the evidential weight of an electronic record, regard shall be had to
- *(a)* the reliability of the manner in which the electronic record was generated, stored or communicated;
- *(b)* the reliability of the manner in which the integrity of the information was maintained;
- *(c)* the manner in which the originator was identified; and
- *(d)* any other relevant factor.

Belize – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2003 Chap 290:01]
****

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

(2) In sections 7, 8, 9, 10 and 11:
- *(a)* where rules of law require information to be in writing, given, signed, original, or retained, the requirement is met if the section is complied with;
- *(b)* where rules of law provide consequences where the information is not in writing, given, signed, original, or retained, the consequences are avoided if the section is complied with; and
- *(c)* where rules of law provide consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.

7. (1) A rule of law that requires information to be in writing or to be given in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference. (2) In subsection (1), giving information includes, but is not limited to, the 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 cancelling an election;
- *(i)* filing or lodging an objection;
- *(j)* giving a statement of reasons.

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

8. A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in 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 so as to be usable for subsequent reference; and
- *(c)* capable of being retained by the other person.

9. (1) If a rule of law requires the signature of a person, that requirement is met by an electronic signature.

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

10. A rule of law that requires a person to produce, examine or keep an original document is satisfied if the person produces, examines or retains the document in electronic form, if
    (a) having regard to all the relevant circumstances, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
    (b) in a case where an original document is to be given to a person, the document given to the person in electronic form is accessible so as to be usable for subsequent reference and capable of being retained by the person.

11. A rule of law that requires a person to keep information either that is in writing or that is in electronic form, is satisfied by keeping the information in electronic form, if :
    (a) having regard to all the relevant circumstances when the electronic form of the document was generated, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
    (b) when the electronic form of the document was generated, the information contained in the electronic form of the document is accessible so as to be usable for subsequent reference to any person entitled to have access to the information or to require its production.

12. For the purposes of sections 10 and 11, the integrity of information in a document is maintained if, and only if, the information has remained complete and unaltered, apart from:
    (a) the addition of any endorsement; or
    (b) any immaterial change, which arises in the normal course of communication, storage or display.

Dominica – NONE

Dominican Republic – GOOD
****

(INFORMAL TRANSLATION)

Article 4-Legal Recognition of Digital Documents and Message Data. Do not refuse legal effects validity or enforceability of all kinds of information by the sole ground that it is in the form of digital document or message data.

Article 5-Record by Writing. When any standard requires that information be recorded in writing, said requirement will be satisfied with a digital document or of a data message if the information it contains is accessible for subsequent consultation and if the document Digital or data message complies with the requirements of validity laid down in this law. The provisions in this article applies whether the requirement laid down by any standard is an obligation, as if the rules provide for consequences in the event that the information not recorded in writing.

Article 6-Signature. Where any rule requires the presence of a signature or establish certain consequences in the absence of the same shall be satisfied this requirement in relationship with a digital document or a data message if It has been digitally signed and complies with the digital signature with the requirements of validity in the present Act.

In any interaction with a public entity that requires signed document, this requirement may meet with one or more digital documents or messages of data that are digitally-signed in accordance with the requirements contained in this Act. The regulation of This law shall specify in detail the conditions for the use of digital signatures, certificates and certification of certification in documentary interactions between entities the State or private persons and State bodies. It provisions of this article shall apply whether the any standard requirement is a obligation, as if the rules simply provided for consequences in the event that there is no signature.

Section VII

Article 7-Original. Where any rule requires that the information is presented and preserved in its form original, that requirement is met with a document Digital or a data message if:

(a) there is a reliable guarantee that has survived the integrity of the information, the date on which was generated for the first time its final form, as digital document, data or other message;

(b) require that information be presented, if This information can be displayed to the person who It must be presented.

In this article applies whether the requirement in any standard is a obligation, as if the rules simply provided for consequences in the event that the information is not presented or retained in its original form.

Art. 8.-Integrity of the Digital Document or Message Data. For the purposes of the preceding article, shall be deemed that the information contained in a digital document or messages database is full, if it has been completed and unchanged, except for the addition of any endorsement or any change that is inherent in the process of communication, file or presentation. The required degree of reliability It shall be determined in the light of the purposes for which it the information generated and all the circumstances relevant to the case.

Article 9.-Admissibility and Evidential Value of the Documents Digital and Message Data. Digital documents and data messages will be admissible as evidence and they will have the same evidential value attached to the acts under private signature in the Civil Code and the code of Civil procedure.

In administrative or judicial proceedings no be denied effectiveness, validity or enforceability and evidence to any type of information in the form of document digital or message data, by the mere fact of it is a digital document or a data message or by reason of having been submitted in its form original.

Article 10.-Criteria for Assessing Appropriateness of a Document Digital or Message Data. To assess the force stages of a project. law on electronic commerce, Documents and digital signatures. Document digital or message data shall be present the reliability of the manner in that has been generated, filed or communicated the digital document or message, the reliability of the form that has preserved the integrity of the information, the way in which identifies its creator or initiator and any other relevant factor.

Article 11.-Preservation of Digital Documents and Messages of Data. When the law requires that certain documents, records or information be retained, that requirement You will be satisfied through the conservation of the digital documents and/or data messages that are of the case, provided that they comply with the following conditions:

1. That the information they contain is accessible to your subsequent consultation;
2. Digital documents or data messages are preserved in the format that is generated, sent received or in a format that allows to show that produces exactly the information originally generated, sent or received;
3. In the case of the message of data is preserved for have any, any information to determine the origin, destination, date and time that was sent or received the message, and
4. In the case of digital document that is preserved for legal purposes, all information to determine the date and time that the digital document was delivered to its conservation, the person or persons who created the document, the person who submitted the document and the person recipient of the same for conservation.

The information which has the sole purpose facilitate access to the digital document or shipment or receipt of data messages should not be subject to the obligation of conservation, except information associated with a data message which constitutes proof of its transmission from its origin to its destination, including but not limited to the message routing within the respective data network, its unique sequential number and the dates and exact times of reception and retransmission and Universal identifiers for each server or node of communications that are involved in the transmission the original message.

Article 12-Conservation of Digital Documents and Messages of Data by a Third Party. The fulfilment of the obligation to preserve documents, records or information in data messages may be perform by a third party, provided that they comply with the conditions set forth in the preceding article.

Grenada* – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Bill, 2008]
****

7. For the purposes of any law [in force in Grenada] information electronic shall not be denied legal effect, validity or admissibility solely on the documents. ground that it is –
   (a) in the form of an electronic document;
   (b) communicated by electronic means; or
   (c) referred to but not contained in the electronic document purporting to give rise to that legal effect, if the information referred to is known to and accepted by the party against whom it is relied upon.

8. (1) Where any law requires information to be in writing, or refers to written information, any such information that is given shall be taken to be given in writing if
   (a) when the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and
   (b) where the information is to be given to the Government and the Government requires that
      (i) the information be given in a particular way in accordance with particular technology requirements; or
      (ii) particular action be taken to verify the receipt of the information, the Government's requirement has been met; and
   (c) where the information is to be given to a person other than the Government, that person consents to the information being given by means of an electronic communication.

(2) This section applies to a requirement or permission to give information, whether or not any of the words "give", "send", "serve" or any other word is used to designate the requirement or permission.

(3) This section does not affect the operation of any other law that makes provision for or in relation to requiring or permitting information to be given, in accordance with particular information technology requirement
   (a) on a particular kind of data storage device; or
   (b) by means of a particular kind of electronic communication.

(4) For the purposes of this section "giving information" includes the following
   (a) making an application;
   (b) making or lodging a claim;
   (c) giving, sending or serving a notice;
   (d) lodging a return;
   (e) making a request;
   (f) making a declaration;
   (g) lodging or issuing a certificate;

(h) making, varying or cancelling an election;
(i) lodging an objection;
(j) giving a statement of reasons.

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

9. Unless otherwise provided by law, parties to a transaction may agree to use of a particular method or form of electronic signature.

10. (1) Where a law requires a person's signature other than a signature of a witness, that requirement is met by means of an electronic signature if the information is given electronically and –
(a) the electronic signature
(i) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates;
(ii) is as reliable as is appropriate having regard to the purpose for which and the circumstances in which, the signature is required, including any relevant agreement;
(b) in the case of a signature on information to be given to a person, that person consents to receiving the electronic signature.

(2) Subject to subsection (3), an encrypted 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 the person can maintain under his sole control;
(d) linked to the information to which it relates in such a manner that any subsequent alteration of the information or the signature is detectable.

(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 an encrypted signature or other method of indicating identity and approval;
(b) adduce evidence of the unreliability of an encrypted signature.

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

(5) In determining whether or to what extent, a certificate or an encrypted signature is legally effective, no regard shall be had to the geographic location
(a) where the certificate is issued or the encrypted signature is created or used; or
(b) of the place of business of the certification service provider or signatory.

(6) This section shall not affect the operation of any other law that requires
(a) information that is given electronically to contain
(i) an encrypted signature(however described);
(ii) a unique identification in an electronic form; or
(b) a particular method to be used for information that is given electronically to identify the originator and to show that the originator approved the information given.

…

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

(a) having regard to all the relevant circumstances at the time, the method of generating the information electronically provided a reliable means of assuring that the integrity of the information is maintained;
(b) when the 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 information is to be produced to
(i) the Government and the Government requires that an electronic form of the document be produced in a particular way, in accordance with particular information technology requirements or that particular action be taken to verify receipt of the document, the Government's requirement is met; or
(ii) any other person, that person consents to the document being produced electronically.

(2) Where a law requires comparison of a document with an original document, that requirement is met by comparing the document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document.

(3) For the purposes of subsection (1) (a) and (2), the criteria for assessing integrity are –
(a) that the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
(b) the purpose for which the information is produced; and
(c) any other relevant factor.

15. (1) Where any law requires a person to retain information for keeping (whether or not in its original form, in writing or in electronic form) for a specified period, that requirement is satisfied by keeping the information in electronic form if the following conditions are satisfied
(a) when the information was first generated in electronic form, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference;
(b) having regard to all the relevant circumstances when the information was first generated in electronic form, the method of retaining the information in that form provided a reliable means of assuring the maintenance of the integrity of the information so generated;
(c) the traffic data relating to the information is also kept in electronic form during the specific period;
(d) when the traffic data was first generated in electronic form, it was reasonable to expect that it would be readily accessible to be useable for subsequent reference; and
(e) if the law requires the information to be kept in electronic form on a particular form of data storage medium, that requirement is satisfied 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 specified that subsection are satisfied.

16. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility in evidence of any information given electronically
(a) solely on the ground that the information is given electronically; or
(b) if the information is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that the information is not in its original form.

(2) Information in the form of an electronic record shall be given due evidential weight and In assessing the evidential weight of an electronic record, regard shall be had to
(a) the reliability of the manner in which
(i) the electronic record was generated, stored or communicated;

(ii) the integrity of the information was maintained;
(c) the manner in which the originator was identified; and
(d) any other relevant factor.

[(3) This section shall not affect the application of the relevant provisions of the [Evidence Act] relating to the admissibility of computer generated evidence.]

17. (1) Where any law requires or refers to serving or delivering information, that information shall be taken to have been served or delivered, as the case may be, if
(a) the information is contained in an electronic document sent to the person upon whom such service or delivery is required to be effected; and
(b) that person acknowledges the receipt of the information.

(2) Nothing in this section affects any rule relating to the time for service or delivery of information.

18. Where any law requires a person to provide information in a p8escribed non electronic form, the Minister responsible may make regulations providing for 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 so as to be useable for subsequent reference; and capable of being retained by the other person.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD – Comprehensive language utilized to effect policy best practice
[Telecommunications Act, 2006]
****

6. For the purposes of any law, information shall not be invalid or inadmissible solely on the ground that the information –
(a) is created, stored or communicated electronically, or
(b) is referred to but is not contained in an electronic document, if the information being referred to is known to and accepted by the party against whom it is relied upon.

7. (1) Where any law requires, or refers to, the giving of information in writing, information that is given electronically shall be taken to be given in writing if –
(a) when the information was given, it was reasonable to expect that the information would be readily accessible to, and capable of retention for subsequent reference, by the addressee;
(b) where the information is to be given to the Government and the Government requires –
(i) that the information be given in a particular way in accordance with particular technology requirements; or
(ii) that particular action be taken to verify the receipt of the information, The Government requirement has been met; and
(c) Where the information is to be given to a person other than the Government, that person consents to the information being given electronically.

(2) This section applies to a requirement or permission to give information whether or not any of the words “give”, “send”, “serve”, or any other word, is used to designated the requirement or permission.

(3) For the purposes of this section, “the giving of information” includes –
(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) lodging or issuing a certificate;
(h) lodging an objection;
(i) giving a statement of reasons.

(4) Where a law referred to in subsection (1) requires more than one copy of the information to be submitted to a person, that requirement shall be taken to have been satisfied by giving the information to the person electronically in accordance with the provisions of this section.

8. (1) A law requiring a person's signature in relation to any information shall be taken to have been met where the information is given electronically and –
(a) a method is used to identify the person and to show the person's approval of the information given;
(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 information was communicated;
(c) if the signature is required to be given to the Government and the Government requires that the method used be in accordance with particular technology requirement, the Government requirement has been met; and
(d) if the signature is required to be given to a person other than the Government, that person consents to that requirement being met by using the method mentioned in paragraph (a).

(2) Subject to subsection (3), an encrypted 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 by identifying that person;
(c) created by using means that such person can maintain under his sole control; and
(d) linked to the information to which it relates in such a manner that any subsequent alteration of the information 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 an encrypted signature or other method of indicating identity and approval;
(b) adduce evidence of the unreliability of an encrypted signature

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

(5) In determining whether, or to what extent, a certificate or an encrypted signature is legally effective, no regard shall be has to the geographic location –
(a) where the certificate is issued or the encrypted signature is created or used; or
(b) of the place of business of the certificate service provider or signatory.

(6) This section shall not affect the operation of any other law that requires –
(a) information that is given electronically to contain an encrypted signature (however described)
(b) information that is given electronically to contain a unique identification in an electronic form; or
(c) a particular method to be used for information that is given electronically to identify the originator and to show that the originator approved the information given.

Section VII

9. Where any law requires a document or signature to be made, attested, acknowledged, authenticated, notarized or verified, or to be made under oath, by any person, that requirement is met if the following are attached to or logically associated with the document –
   (a) the encrypted signature of that person;
   (b) in the case of a signature or a document 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 document; and
   (d) all other information required to be included under any other law.

10. (1) Where any law requires or permits information to be presented in its original form, or to be made available for inspection, that requirement is met where the information is produced electronically if –
   (a) having regard to all the relevant circumstances at the time, the method of producing the information electronically provided a reliable means of assuring the maintenance of the integrity of the information;
   (b) when the 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 information is to be produced to the Government and the Government requires that –
      (i) an electronic form of the document be produced is a particular way, in accordance with particular information technology requirements; or
      (ii) particular action be taken to verify receipt of the document

   The Government's requirement has been met; and

   (d) where the document is to be produced to a person other than the Government, that person consents to the document being processed electronically

(2) For the purposes of subsection (1)(a), the criteria for assessing integrity are –
   (a) that the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
   (b) the purpose for which the information is produced; and
   (c) any other relevant factor.

11. (1) Where any law requires a person to keep information (whether or not in its original form, in writing or in electronic form) for a specified period, that requirement is met by keeping information electronically if the following conditions are satisfied –
   (a) when the information was first generated in electronic form, it was reasonable to expect that the information would be readily accessible so as to be useable or subsequent reference;
   (b) having regard to all the relevant circumstances when the information was first generated in electronic form, the method of retaining the information in electronic form provided a reliable means of assuring the maintenance of the integrity of the information that was generated;
   (c) the traffic data relating to the information 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 to be kept in electronic form on a particular kind of storage medium, that requirement is met throughout the specified period.

Section VII

(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.

12. (1) In any legal proceedings, nothing in the rules or evidence shall apply so as to deny the admissibility in evidence of any information given electronically –
(a) solely on the ground that the information is given electronically; or
(b) if the information is the best evidence that the person adducing it could reasonably be expected to obtain , on the ground that the information is not in its original form.

(2) In assessing the evidential weight of the information given electronically, regard shall be has to –
(a) the reliability of the manner in which the information was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the information was maintained;
(c) the manner in which the originator was identified; and
(d) any other relevant factor.

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED
[Electronic Transactions Bill, 2007]
****

13. A legal requirement can be satisfied using information technology where sections 16 to 32 and the conditions or the Regulations are satisfied.
…

15. For the purposes of this Part, the integrity of information is maintained only if the information has remained complete and unaltered, other than the addition of an endorsement, or ant [immaterial change], that arises in the normal course of communication, storage or display.

16. A legal requirement that information be in writing is satisfied by information that is in electronic form if the information is accessible so as to be usable for subsequent reference.

17. a legal requirement that information be recorded in writing is satisfied by recording the information in electronic form if the information is accessible so as to be usable for subsequent reference.

18. (1) A legal requirement to give information in writing is satisfied by information in electronic form, whether by means of electronic communication or otherwise, if –
(a) the information is accessible so as to be usable for subsequent reference;
(b) the person to whom the information is required to be given consents to the information being given in electronic form and by means of an electronic communication, if applicable; and
(c) the information is capable of being retained by the person to whom it is given

(2) where subsection (1) applies, a legal requirement to provide multiple copies of the information to the same person at the same time is satisfied by providing a single electronic version of the information.

(3) In subsection (1), giving 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 cancelling an election;
(i) filing or lodging an objection;
(j) giving a statement of reasons.

19. A legal requirement that a person provides information in a prescribed non-electronic form to another person is satisfied by the provision of the information 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 so as to be usable for subsequent reference; and
(c) capable of being retained by the other person.

…

24. (1) A legal requirement to retain information that is in paper or other non-electronic form is satisfied by retaining an electronic form of the information if-
(a) the electronic form provides a reliable means of assuring maintenance of the integrity of the information; and
(b) the information is readily accessible so as to be usable for subsequent reference.

Saint Vincent and the Grenadines – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2007]
****

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

(2) In sections 5, 6, 7, 8 and 22:
(a) where a rule of law require information to be in writing, given, signed, original or retained, the requirement is met if the section is complied with;
(b) where a rule of law provides consequences where the information is not in writing, given, signed, original or retained, the consequences are avoided if the section is complied with; and
(c) where a rule of law provides consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.

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

(2) In subsection (1), giving information includes, but is not limited to, the 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 cancelling an election;
(i) filing or lodging an objection;
(j) giving a statement of reasons.

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

Section VII

6. (1) A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in 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 so as to be usable for subsequent reference;and
   (c) capable of being retained by the other person.

7. A rule of law that requires a person to produce, examine or keep an original document is satisfied if the person produces, examines or retains the document in electronic form, if:
   (a) having regard to all the relevant circumstances, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
   (b) in a case where an original document is to be given to the person in electronic form is accessible so as to be usable for subsequent reference and capable of being retained by the person.

8. A rule of law that requires a person to keep information that is in writing or that is in electronic form, is satisfied by keeping the information in electronic form, if:
   (a) having regard to all the relevant circumstances when the electronic form of the document was generated, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
   (b) when the electronic form of the document was generated, the information contained in the electronic form of the document is accessible so as to be usable for subsequent reference to any person entitled to have access to the information or to require its production.

9. For the purposes of sections 7 and 8 the soundness of the information has remained complete and unaltered, apart from:
   (a) the addition of any endorsement; or
   (b) any immaterial change;

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

10. (1) If a public authority has power to create, collect, receive, store, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the power to do so electronically.

(2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

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

(4) Where a public authority consents to receive any information in electronic form, it may specify:
   (a) the manner, and format in which the information shall be communicated to it;
   (b) the type or method of electronic signature required, if any;
   (c) control processes and procedures to ensure integrity, security and confidentiality of the information;
   (d) any other attributes for the information that are currently specified for corresponding information on paper.

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

Section VII

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

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

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

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

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

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

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

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

Suriname – NONE

Trinidad and Tobago – LIMITED (GOOD) – Enabling language utilized to effect policy best practice comprehensively.
[Electronic Transactions Bill, 2009]
****

8. An electronic data message, record or information to which this Act applies shall not be denied legal effect or enforceability merely because it is in electronic form.

9. The legal requirement that a record, a data message, or some particular information be in writing is satisfied where that record, data message or information is presented in electronic form, if the electronic record, data message or information is accessible and capable of retention for subsequent reference.

10. (1) The legal requirement that information, a data message or a record be provided or sent to a person may be met by providing or sending the information, data message or record by electronic means.

Section VII

(2) For the purpose of this Act, information, a data message or a record is not provided or sent to a person if it is merely made available for access by the person or is not capable of being retained.

11. Where a written law requires information, a data message or a record to be presented in a specified non-electronic form, that requirement is satisfied if the information, data message or record in electronic form–
(a) is organized in substantially the same way;
(b) is accessible; and
(c) is capable of retention for subsequent reference.

12. (1) Where a written law requires information, a data message or a record to be presented or retained in its original form, that requirement is satisfied by the information, data message or record being presented in electronic form if–
(a) there exists a reliable assurance as to the maintenance of the integrity of the information, data message or record by the person who presented the information;
(b) it is presented to a person; and
(c) the information, data message or record in electronic form is accessible and capable of retention for subsequent reference.

(2) The criterion for assessing integrity under subsection (1) shall be whether the information, data message or record has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display.

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

13. Where a written law requires that certain information, data messages or records be retained, that requirement is satisfied by retaining information, data messages or records in electronic form.

14. Information, a data message or a record in electronic form is not capable of being retained if the person providing the information, data message or record prevents or does anything to hinder its printing, audio or video playback or storage by the recipient.

15. Where information, a data message or a record is provided in electronic form, a requirement under any written law for one or more copies of the information or record to be provided to a single addressee at the same time is satisfied by providing a single copy in electronic form.

16. A copy of an electronic data message containing an electronic signature shall be as valid, enforceable and effective as a message containing a non-electronic signature.

17. An electronic data message or record will not be deemed inadmissible as evidence–
(a) solely on the ground that it is in electronic form; or
(b) on the ground that it is not in the original non-electronic form, if it is the best evidence.

Section VII

International Best Practice and Regional Trends

1. OECS Model Law

****

Satisfaction of Legal Requirements Through Use of Electronic Technology

11. A legal requirement can be met using electronic technology if-
    (a) the provisions in subpart 2 are satisfied; and
    (b) any conditions prescribed by the Regulations are satisfied.

....

When Integrity of Information Maintained

13. For the purposes of this Part, the integrity of information is maintained only if the information has remained complete and unaltered, other than the addition of any endorsement, or any immaterial change, that arises in the normal course of communication, storage, or display.

Requirement that Information be in Writing

14. A legal requirement that information be in writing is met by information that is in electronic form if the information is readily accessible so as to be usable for subsequent reference.

Requirement to Record Information in Writing

15. A legal requirement that information be recorded in writing is met by recording the information in electronic form if the information is readily accessible so as to be useable for subsequent reference.

Requirement to Give Information in Writing

16.(1) A legal requirement to give information in writing is met by giving the information in electronic form, whether by means of an electronic communication or otherwise, if–
    (a) the information is readily accessible so as to be usable for subsequent reference; and
    (b) the person to whom the information is required to be given consents to the information being given in electronic form and by means of an electronic communication, if applicable.

(2) If sub-section (1**)** applies, a legal requirement to provide multiple copies of the information to the same person at the same time is met by providing a single electronic version of the information.

(3) Sub-section (1) applies to a legal requirement to give information even if that information is required to be given in a specified manner, for example by filing, sending, serving, delivering, lodging, or posting that information.

(4) Legal requirement to give information includes, for example, -
    (a) making an application;
    (b) making or lodging a claim;
    (c) giving, sending, or serving a notification;
    (d) lodging a return;
    (e) making a request;
    (f) making a declaration;
    (g) lodging or issuing a certificate;
    (h) making, varying, or canceling an election;
    (i) lodging an objection;
    (j) giving a statement of reasons.

Section VII

Additional Requirements Relating to Information in Writing

17. To avoid doubt, a legal requirement relating to the form or layout of, or the materials to be used for writing, information, or any similar requirement, need not be complied with in order to meet a legal requirement to which any of sections 18 to 20 apply.

…

Originals

28. A legal requirement to compare a document with an original document may be met by comparing that document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document.

2. UNCITRAL Model Law

****

Chapter II. Application of Legal Requirements to Data Messages

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforce- ability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference
(as adopted by the Commission at its thirty-first session, in June 1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

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

(3) The provisions of this article do not apply to the following: [...].

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and Evidential Weight of Data Messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of Data Messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Section VII

7.4 Contract Formation

International Best Practices and Regional Trends

- The framework outlines how the source of an electronic document is to be attributed
- The framework outlines how the time of sending or receipt of an electronic document is established
- The framework outlines how the place of residence or work of either party in a transaction is established
- The framework outlines requirements for treating with corrections of errors in a valid electronic contract.

Antigua and Barbuda – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Bill 2006]

****

16. (1) In the context of the information of a contract -

(a) an offer;

(b) subject to any condition included in the offer (notwithstanding section 2), the acceptance of an offer; and

(c) the method of payment of any consideration payable, may be expressed by an electronic record.

(2) As between the originator and the addressee of an electronic record, a declaration of intention or other statement shall not be denied legal effect or validity solely on the ground that it is in the form of an electronic record.

17. (1) An electronic record is that of an originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record shall be attributable to the originator if it was sent -

(a) by a person who had been authorized by the originator to send the electronic record on his behalf; or

(b) by the originator's electronic agent.

(3) 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.

(4) Subsection (3) 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 (3)(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.

Section VII

(5) 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.

18. If a change or error occurs in the transmission of an electronic record -

(a) If the originator and the addressee have agreed to use an information security procedure in respect of the electronic record and one of them has conformed to the procedure, but the other has not, and the nonconforming person would have detected the change or error had he also conformed, the conforming person may avoid the effect of the changed or erroneous electronic record;

(b) if an individual is either the originator or the addressee of an electronic record, he may avoid the effect of the electronic record if the error was made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual-

(i) promptly notifies the other person of the error and that he did not intend to be bound by the electronic record received by the other person;

(ii) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(iii) has not used or received any benefit or value from the consideration, if any, received from the other person; and

(c) if neither paragraph (a) nor paragraph (b) applies, the change or error shall have the effect provided by any other law and any contract between the originator and the addressee;

19. (1) Subscriptions (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested, or agreed with, the addressee that receipt of the electronic record be acknowledged by the addressee.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –

(a) a communication by the addressee to the originator, automated or otherwise; or

(b) the conduct of the addressee, that is reasonably sufficient to indicate to the originator, the electronic record has been received.

(3) Where the originator has stated that an electronic record is conditional, on receipt by him of an acknowledgement, the record shall be presumed not to have been sent until an acknowledgment has been received by him.

(4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator -

(a) may give notice to the addressee –

(i) stating that no acknowledgement has been received and that the electronic record is to be treated as though it had never been sent; or

(ii) specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee –

(i) treat the electronic record as though it had never been sent; and

(ii) exercise any other rights the originator may have.

(5) Where the originator receives the addressee's acknowledgement of receipt it may be presumed that the related electronic record has been received by the addressee but that presumption shall not imply that the electronic record received corresponds to the electronic record as sent.

(6) Where the addressee's received acknowledgment states that the related electronic record met technical requirements that the originator and the addressee have agreed should be met, it shall be presumed that the requirements have been met.

(7) Except in so far as it relates to the sending or receipt of an electronic record, this section shall not affect the legal or equitable consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

20. (1) Unless the originator and addressee agree otherwise, information place or a record in electronic form is sent when it enters an information system outside the control of the originator or, if the originator and the addressee are in the same information system, if the information or record becomes capable of being retrieved and processed by the addressee.

(2) If information or a record is capable of being retrieved and processed by an addressee, the information or record in electronic form is deemed, unless the contrary is proven, to be received by the addressee-

(a) when it enters an information system designated or used by the addressee for the purpose of receiving information or records in electronic form of the type sent, or

(b) if the addressee has not designated or does not use an information system for the purpose of receiving information or records in electronic form of the type sent, on the addressee becoming aware of the information or record in the addressee's information system.

The Bahamas – GOOD – Comprehensive language utilized to effect policy best practice.

[Electronic Communications and Transactions Act 2003]

****

13. In the context of formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic communications.

14.(1) An electronic communication is attributable to a person if the electronic communication resulted from the action of the person, acting in person, by his agent, or by his electronic agent device.

(2) Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic communication was attributable.

(3) An addressee is not entitled to regard the electronic communication received as being what the originator intended to send where the addressee knew or ought reasonably to have known, had he exercised reasonable care or used an agreed procedure, that the transmission resulted in any error in the electronic communication as received.

(4) Nothing in this section affects the law of agency or the law on the formation of contracts.

15.(1) Where the originator of an electronic communication has stated that the electronic communication is conditional upon receipt of an acknowledgement –

(a) the electronic communication is to be treated as though it had never been sent until the acknowledgement is received;

(b) if there is no agreement between the originator and the addressee as to the particular form or method of the acknowledgement to be given, the addressee may give an acknowledgement by any means of communication automated or otherwise or by any conduct that is reasonably sufficient to indicate to the originator that the electronic communication has been received.

(2) Where the originator indicates that receipt of an electronic communication is required to be acknowledged but has not stated that the electronic communication is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator -

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the electronic communication as though it had never been sent or exercise any other rights the originator may have.

(3) Where the received acknowledgement states that the related electronic communication met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(4) Except in so far as it relates to the sending or receipt of the electronic record, this section is not intended to deal with the legal consequences that may flow either from that electronic communication or from the acknowledgement of its receipt.

16. Where any statutory or legal requirement exists for a document to-be notarized, verified, or made under oath, that requirement is met if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

17.(1) Where information is required by law to be delivered, dispatched, given or sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic communication provided that the originator of the electronic communication states that the receipt of the electronic communication is to be acknowledged and the addressee has acknowledged its receipt.

(2) Subsection (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

(3) Subject to section 5, the dispatch of an electronic communication occurs when it enters an information processing system outside the control of the originator.

(4) Subject to section 5, the time of receipt of an electronic communication is determined as follows -

(a) where the addressee has designated an information processing system for the purpose of receiving electronic communications, receipt occurs -

(i) at the time when the electronic communication enters the designated information processing system; or

(ii) if the electronic communication is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic communication comes to the attention of the addressee;

(b) where the addressee has not designated an information processing system, receipt is deemed to have occurred on the earlier happening of -

(i) the time at which the electronic communication enters an information processing system of the addressee; or

(ii) otherwise comes to the attention of the addressee.

(5) Subsection (4) shall apply notwithstanding that the place where the information processing system is located may be different from the place where the electronic communication is deemed to be received under subsection (6).

(6) Unless otherwise agreed between the originator and the addressee, an electronic communication is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(7) For the purposes of subsection (6) –

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic communication relates or, where there is no such transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

18.(1) The generation of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

(2) The production, by means of an electronic communication, of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

Barbados – FAIR – Comprehensive language utilized to effect policy best practice on issues of attestation, sending and receipt of electronic documents. There are no explicit provisions regarding correction of errors.

[Electronic Transactions Act, CAP. 308B]

****

12. (1) Unless otherwise agreed by the parties, an offer, and the acceptance of an offer, in relation to the formation of a contract may be expressed by means of electronic records.

(2) Where an electronic record is used in the formation of a contract, that contract shall not be denied legal effect, validity or enforceability solely on the ground that an electronic record was used for that purpose.

13. As between the originator and the addressee of an electronic record, a declaration of intention or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

14. (1) An electronic record is attributable to a person if the electronic record resulted from the action of the person, his agent, or his electronic device.

(2) As between the originator of the electronic record and the addressee of that record, an addressee is entitled to regard an electronic record as being that of the originator, and to act on that assumption where

(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 the electronic record as his own.

(3) Subsection (2) does not apply

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

(4) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic record as received as being what the originator intended to send, and to act on that assumption; but the addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in an error in the electronic record as received.

(5) The addressee is 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 the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

15. (1) Subsections (2), (3) and (4) apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record is to be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee that is reasonably sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgment, the electronic record is to be treated as though it had never been sent until the acknowledgment is received.

(4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, where no time has been specified or agreed, within a reasonable time, the originator

(a) may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and

(b) if the acknowledgment is not received within the time specified in paragraph *(a)*, may, upon notice to the addressee, treat the electronic record as though it had never been sent or exercise any other rights the originator may have.

(5) Where the originator receives the addressee's acknowledgment of receipt, it is presumed that the related electronic record was received by the addressee, but that presumption does not imply that the electronic record corresponds to the record received.

(6) Where the acknowledgment of receipt of the addressee states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

Section VII

(7) Except in so far as it relates to the sending or receipt of the electronic record, this section is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgment of its receipt.

16. (1) Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information-processing system outside the control of the originator, or his agent.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(a) where the addressee has designated an information processing system for the purpose of receiving electronic records, receipt occurs

(i) at the time when the electronic record enters the designated information-processing system, or

(ii) if the electronic record is sent to an information-processing system of the addressee that is not the designated information-processing system, at the time when the electronic record is retrieved by or comes to the attention of the addressee;

(b) where the addressee has not designated an information processing system, receipt occurs when the electronic record enters an information-processing system of the addressee or otherwise is retrieved by or comes to the attention of the addressee.

(3) Subsection (2) applies notwithstanding that the place where the information-processing system is located may be different from the place where the electronic record is deemed to be received under subsection (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(5) For the purposes of subsection (4)

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic record relates or, where there is no transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

Belize – GOOD – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Act, 2003 Chap 290:01]

****

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

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

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

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

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

Section VII

20. (1) An electronic transaction between an individual and another person's automated source of information has no legal effect if :
(a) the individual makes a material error in electronic information or an electronic document used in the transaction;
(b) the automated source of information does not give the individual an opportunity to prevent or correct the error;
(c) on becoming aware of the error, the individual promptly notifies the other person; and
(d) in a case where consideration is received as a result of the error, the individual, returns or destroys the consideration in accordance with the other person's instructions or, if there are no instructions, deals with the consideration in a reasonable manner, and does not benefit materially by receiving the consideration.

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

21. As 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.

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

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

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

(5) If the sender or the addressee has more than one place of business, the place of business for the purposes 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).

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

Dominica – NONE

Section VII

Dominican Republic – GOOD
****

(INFORMAL TRANSLATION)

Article 13. Formation and Validity of the Contracts. In the formation of the contract, unless expressly agreed between the parts, supply and acceptance may be expressed by means of a digital document, a data message, or a data bearer of a digital document message, as It is the case. Not be denied validity or enforceability to a contract on the sole ground of having been used in its training one or more digital documents or messages of data.

Article 14. Recognition of Digital Documents and Messages of Data by the Parties. In the relations between the originator and the addressee's a message database, or between the signatories of a document digital, where any, they shall not be denied legal effect, validity or binding to a manifestation of will or other statement by the single Why have been made in the form of digital document or message data.

Article 15. Communication and Allocation of Digital Documents. A digital document can communicate between parties, already either by the delivery of the digital document in a physical environment a party to the other, or a data message that, in addition to its own content, include a true, verifiable representation of digital document.

Means that a digital document comes in the person or persons to sign digitally the document, regardless of the support that is encumbered such document and of the means of communication. In the case of transmission of the digital document by message of absence of internal to the document digital signature and data are It means that the digital document comes from the initiator the message of data in accordance with article 16 of the present Act.

Article 16. Power of a Data Message. Means that a data message comes from the originator, when it has been submitted by:

1. The originator himself;
2. By any person authorized to act on behalf of the Initiator on that message, or
3. For an information system programmed by the initiator, or on its behalf, that operates automatically.

Article 17. Presumption of the Origin of a Data Message. It is presumed that a data message has been sent by the initiator and, therefore, the recipient can work in as a result, when:

1 Has properly applied the procedure previously agreed with the originator, to establish that the data message actually came from, and

2. The data message received by the recipient is the acts of a person whose relationship with the originator, or with any agent you given access to some method used by the originator to identify a data message as its own.

…

Article 22. Presumption of Receipt of a Data Message. When the initiator receives acknowledge of receipt of the recipient, shall be presumed that it has received the message data. This presumption does not imply that the message of data corresponds to the received message. When in the acknowledgement of receipt indicates that the received data message It meets the technical requirements agreed upon or set forth any applicable technical standard, it shall be presumed that it is the case.

Article 23. Effects Legal. Articles 20, 21 and 22 of the This Act govern only the related effects with the acknowledgement of receipt. The legal consequences of the document digital or of a data message shall be governed in accordance with the rules applicable to the Act or legal business content in the digital document or data message.

Section VII

Article 24. Time of the Sending of a Message's Data. Of no agree on one thing the originator and the addressee, the data message will be dispatched when you log in an information system that is not under the control of the originator or of the person who sent the data message in the name of it.

Article 25. Time of the Receipt of a Message's Data. Of unless another thing the originator and the addressee, the time of receipt of a data message is It shall be determined as follows:

(a) if the addressee has designated a system of information for the reception of data message, the reception will take place:
   1. At the time they enter the data message in the designated information system;
   2. To send the data message to a system of information of the addressee that is not the system of information designated at the time when the addressee retrieve the data message.

(b) if the addressee has not designated a system of information, reception will take place when the message of data type to a system of information of the recipient.

In this article shall apply even When is the information system located in place other than where you received the message of data According to the following article.

Article 26. Place of Dispatch and Receipt of the Data Message. Unless otherwise the originator and the addressee, the data message shall be dispatched at the place where the originator has its place of business, and shall be taken by received at the place where the addressee has yours.

For the purposes of this article:

(a) if the originator or recipient has more than one establishment, its establishment is that closest one relationship to the underlying transaction, or, not have an underlying transaction, its establishment main;

(b) if the originator or the addressee does not have establishment, it shall take into account their place of residence usual.

Grenada* – LIMITED (GOOD) – Comprehensive language utilized to effect, and elaborate upon policy best practice.

[Electronic Transactions Bill, 2008]

****

20. (1) In relation to the formation of contracts, an offer and the and validity acceptance of an offer may be expressed electronically, unless the of contracts. parties agree otherwise.

(2) As between the originator and the addressee of an electronic document, a declaration of intention or other statement or delivery of a deed shall not be denied legal validity or be unenforceable solely on the ground that it is in an electronic document.

(3) A contract may be formed by the interaction of the automated communications device of each party, even if no individual was aware of or reviewed the actions of the device or the resulting terms and agreements.

(4) Subsection to subsection (5), a contract may be formed by the interaction of an automated communications device and an individual acting on his own behalf or for another person, including an interaction referred to in subsection (5).

Section VII

(5) The interaction mentioned in subsection (4) is one in which the individual performs actions that the individual
(a) is free to refuse to perform; and
(b) knows or has reason to know will cause the device to complete the transaction.

(6) In the circumstances referred to in subsections (4) and (5), the individual or the person on whose behalf the individual is acting, as the case may be, shall not be bound by the terms of the contract unless, prior to the formation of the contract, those terms were capable of being reviewed by the individual.

21. (1) Unless otherwise agreed between the originator and the of addressee of an electronic document, the originator is bound by that electronic document only if the document was sent by him or under his authority.

(2) Subsection (1) shall not affect the operation of a law that makes provision for
(a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or
(b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

(3) An electronic document between an originator and an addressee shall be deemed to be that of the originator if it was sent by an information system programmed to operate automatically by or on behalf of the originator.

(4) As between the originator and the addressee, the addressee shall have the right to assume that an electronic document is being sent by the originator and to act on that assumption if
(a) in order to ascertain whether the document is that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
(b) the document as received by the addressee resulted from the actions of a person whose relationship with the originator enabled that person to gain access to a method used by the originator to identify electronic documents as his own

(5) Subsection (4) does not apply
(a) as of the time when the addressee has received notice from the originator that the electronic document was not sent by the originator and had reasonable time to act accordingly; or
(b) in any case falling within subsection (4)(b), at any time when the addressee knew, or ought to have known had he exercised reasonable care or used any agreed procedure, that the electronic document was not sent by the originator.

(6) An addressee is not entitled to regard an electronic document as being what the originator intended to send if the addressee knew, or ought reasonably to have known had he exercised reasonable care or used an agreed procedure, that
(a) the document was sent in error; or
(b) the transmission of the document resulted in an error in the document as received by the addressee.

(7) The addressee is entitled to regard each electronic document received as a separate document and to act on that assumption, except to the extent that it duplicates another electronic document and the addressee knew or ought reasonably to have known, had he exercised reasonable care or used any agreed procedure, that the electronic document was a duplicate.

Section VII

22. (1) This section applies where a change or error occurs in the change or transmission of an electronic document between parties.

(2) Where there is an agreement between the parties to use a security procedure to detect changes or errors in the electronic document and
- (a) only one of the parties has conformed to the procedure; and
- (b) the non-conforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic document.

(3) A party may avoid the effect of an electronic document that results from an error made by the party in dealing with another person's automated communications device if –
- (a) the device did not provide an opportunity for the prevention or correction of the error; and
- (b) the conditions specified in subsection (4) are applicable.

(4) The conditions mentioned in subsection(3) are that, at the time the party learns of the error, that party
- (a) promptly notifies the person of the error and that the party did not intend to be bound by the erroneous document;
- (b) takes steps that conform to the person's reasonable instructions for the return or disposal of the consideration (if any) received by the party as a result of the erroneous document;
- (c) if no reasonable instructions are given under paragraph (b), takes reasonable steps for the return or disposal of such consideration; and
- (d) has not received any benefit or value form such consideration.

(5) Where neither subsection (2),(3) nor (4) applies, the change or error shall have the effect provided for by a contract between the parties or by law, in the absence of such contract.

(6) The provisions of subsections (2), (3) and (4) may not be varied by agreement.

23. (1) The provisions of this section apply where, on or before sending an electronic document, or by means of that document, the originator requests or agrees with the addressee that receipt of the document is to be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by
- (a) any communication by the addressee, automated or otherwise; or
- (b) any conduct of the addressee that is reasonably sufficient to indicate to the originator that the electronic document has been received.

(3) Where the originator has stated that the electronic document is conditional on receipt of the acknowledgement, the document is to be treated as though it had never been sent until the acknowledgment is received.

(4) Subsection (5) applies in cases where –
- (a) the originator has not stated that the electronic document is conditional on receipt of the acknowledgement; and
- (b) the acknowledgement is not received by the originator within the time specified or agreed, or, where no time is specified or agreed, within a reasonable time.

(5) The originator
- (a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
- (b) if the acknowledgement is not received within the time specified in paragraph (a), may , upon notice to the addressee, treat the electronic document as though it had never been sent or exercise any other rights that the originator may have.

Section VII

(6) An acknowledgement of the receipt given by the addressee to the originator shall be taken as *prima facie* proof that an electronic document was received by the addressee, but nothing in this subsection shall be construed as implying that the electronic document sent corresponds to the electronic document received.

(7) A statement in an acknowledgement of receipt given by the addressee that the related electronic document meets technical requirements, either agreed upon between originator and addressee or set out in applicable standards, shall be taken as prima facie proof that those requirements have been met.

(8) Except in so far as it relates to the sending or receipt of the electronic document, this section shall not affect the legal consequences that may flow either from the electronic document or from the acknowledgement of its receipt.

24. Sections 25 to 27 apply to an electronic communication except to the extent that the parties to the electronic communication otherwise agree.

25. (1) The dispatch of an electronic communication occurs when it enters an electronic communications system outside the control of the originator or his agent.

(2) Where an electronic communication enters two or more electronic communications systems outside the control of the originator, the electronic communication is taken to be dispatched at the time it enters the first of those systems.

26. An electronic communication is taken to be dispatched from
- (a) the originator's place of business; or
- (b) if the originator has more than one place of business
  - (i) the place of business that has the closest relationship with the underlying transaction; or
  - (ii) if there is no place of business to which subparagraph (i) applies, the originator's principal place of business; or
- (c) if the originator has no place of business, the originator's ordinary place of residence.

27. (1) An electronic communication is taken to be received
- (a) if an addressee has designated an electronic communications system for the purpose of receiving electronic communications
  - (i) at the time the electronic communication enters that system; or
  - (ii) if the electronic communication is sent on an electronic communications system other than the system designated by the addressee, at the time when the electronic communication is retrieved by or comes to the attention of the addressee;
- (b) if the addressee has not designated an electronic communications system, at the time when the electronic communication enters an electronic communications system of the addressee or otherwise is retrieved by or comes to the attention of the addressee;

(2) Subsection (1) applies notwithstanding that the place where the electronic communications system is located may be different from the place where the electronic communication is taken to be received under subsection (3).

28. (1) An electronic communication is taken to be received at
- (a) the addressee's place of business; or
- (b) If the addressee has more than one place of business
  - (i) the place of business that has the closest relationship with the underlying transaction; or

(ii) if there is no place of business to which subparagraph (i) applies, the addressee's principal place of business; or

(c) If the addressee has no place of business, the addressee's ordinary place of residence.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD – Comprehensive, prescriptive language utilized to effect, and elaborate upon policy best practice

[Electronic Transactions Act, 2006]

****

16. (1) In the context of the formation of contracts, unless otherwise agreed by parties, an offer and the acceptance of an offer may be expressed electronically.

(2) As between the originator and the addressee of an electronic document, a declaration of intention or other statement or delivery of a deed shall not be denied legal validity or enforceability solely on the ground that it is an electronic document.

(3) A contract may be formed by the interaction of the automated communications device of each party, even if no individual was aware of o reviewed the actions of the device or the resulting terms and agreements.

(4) Subject to subsection (5), a contract may be formed by the interaction of an automated communications device and an individual, acting on the individual's own behalf or for another person, including an interaction in which the individual performs actions that the individual –

(i) is free to refuse to perform; and

(ii) knows or has reason to know will cause the device to complete the transaction.

(5) In the circumstances referred to in subsection (4), the individual or the person on whose behalf the individual is acting, as the case may be, shall not be bound by the terms of the contract unless, prior to the formation of the contract, those terms were capable of being reviewed by the individual.

17. (1) An electronic document is sent by a person (A) if –

(a) as between A and any other person, the document was sent by A himself; or

(b) as between A and the addressee; the document was sent by –

(i) another person who has the authority to act on behalf of A; or

(ii) an automated communications device programmed, by or in behalf of A, to operate automatically.

(2) As between the originator and the addressee, the addressee is entitled to assume that an electronic document is being sent by the originator and to act on that assumption if –

(a) in order to ascertain whether the document is that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the document as received by the addressee resulted from the actions of a person whose relationship with the originator enabled that person to gain access to method used by the originator to identify electronic documents as his own.

(3) Subsection (2) does not apply –

(a) as of the time when the addressee has-

(i) received notice from the originator that the electronic document was not sent by the originator; and

Section VII

(ii) had reasonable time to act accordingly; or

(b) in any case falling within subsection (2)(b), at any time when the addressee knew, or ought to have known had he exercised reasonable care or used any agreed procedure, that the electronic document was not sent by the originator

(4) An addressee is not entitled to regard an electronic document as being what the originator intended to send if the addressee knew, or ought reasonably to have known had he exercised reasonable care or used an agreed procedure, that –

(a) the documents was sent in error; or

(b) the transmission of the document resulted in an error in the document as received by the addressee

…

19. (1) The provisions of this section apply where, on or before sending an electronic document, the originator indicated to the address that the receipt of the document must be acknowledged.

(2) Where, on or before sending the electronic document, the originator indicates to the addressee that the communication of the document is conditional on the receipt of the acknowledgement, the document shall be treated, as between the originator and the addressee, as if the document had never been sent, until the originator receives the acknowledgment.

(3) Where there is no agreement between the originator and the addressee as to the form or method of acknowledgment, the addressee may give the acknowledgement by any means of communication, electronic, automated or otherwise, or by any conduct that is reasonably sufficient to indicate to the originator that the electronic document has been received by the addressee.

(4) Subsection (5) applies where the originator has not indicated, in accordance with subsection (2), that the communication of the electronic document is conditional upon receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the specified or agreed or, if no time has been specified or agreed, within a reasonable time.

(5) The originator –

(a) may give notice to the addressee stating that no acknowledgment as been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the document as though it had never been sent, or exercise any other rights the originator may have.

(6) An acknowledgement of receipt given to the originator by the addressee shall be taken as prima facie proof that an electronic document was received by the addressee, but nothing in this subsection shall be construed as implying that the electronic document sent corresponds to the electronic document received.

(7) A statement in an acknowledgement of receipt given by the addressee that the related electronic document meets technical requirements, either agreed upon between originator and addressee or set forth in applicable standards, shall be taken as prima facie proof that those requirements have been met.

Section VII

(8) Except in so far as it relates to the sending or receipt of the electronic document, this section shall not affect the legal consequences that may flow either from that electronic document or from the acknowledgement of its receipt.

20. (1) Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic document occurs when it enters an electronic communications system outside the control of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic document is determined as follows –

(a) where the addressee has designated an electronic communications system for the purpose of receiving electronic documents, receipt occurs –

(i) at the time when the document enters the designated electronic communications system;

(ii) if the document is sent on an electronic communications system of the addressee that is not the designated electronic communication system, at the time when the document comes to the attention of the addressee;

(b) where the addressee has not designated an electronic communications system, receipt occurs when the document enters an electronic communications system of the addressee or otherwise comes to the attention of the addressee.

(3) Subsection (2) applies notwithstanding that the place where the electronic communications system is located may be different from the place where the electronic document is deemed to be received under subsection (4).

(4) Unless otherwise agreed between the originator and the address, an electronic document is deemed to be dispatched at the originator's place of business, and is deemed to be received at the addressee's place of business.

(5) for the purposes of subsection (4) –

(a) if the originator or the addressee, as the case may be, has more than one place of business, the place of business is that which has the closest relationship to the matter to which the electronic document relates.

(b) if the originator does not have the place of business, the electronic document is seemed to be dispatched at the place where the originator ordinarily resides;

(c) if the addressee does not have the place of business, the electronic document is seemed to be received at the place where the addressee ordinarily resides.

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (GOOD)
[Electronic Transactions Bill, 2007]
****

7. An electronic communication is taken to be dispatched at the time the electronic communication first enters an information system that is outside the control of the originator.

8. An electronic communication is taken to be received –

(a) in the case of an addressee who has designated an information system for the purpose of receiving electronic communications, at the time the electronic communication enters that information system; or

(b) in any other case, at the time the electronic communications comes to the attention of the addressee.

9. An electronic communication is taken to be dispatched from –
(a) the originator's place of business, or
(b) of the originator has more than one place of business;
(i) the place of business that has the closest relationship with the underling transaction; or
(ii) if there is no place of business to which the subparagraph (i) applies, the originator's principal place of business; or
(c) in the case of an originator who does not have a place of business, the originator's ordinary place of residence.

10. An electronic communication is taken to be received at-
(a) the originator's place of business, or
(b) of the originator has more than one place of business;
(i) the place of business that has the closest relationship with the underling transaction; or
(ii) if there is no place of business to which the subparagraph (i) applies, the originator's principal place of business; or
(c) in the case of an originator who does not have a place of business, the originator's ordinary place of residence.

Saint Vincent and the Grenadines – GOOD – Comprehensive language utilized to effect policy best practice.
[Electronic Transactions Act, 2007]
****

16. (1) Unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed:
(a) by means of information in electronic form; or
(b) by an act that is intended to result in electronic communication, such as touching or clicking an appropriate icon or other place on a computer screen, or by speaking.

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

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

18. (1) An electronic transaction between an individual and another person's automated source of information has no legal effect if:
(a) the individual makes a material error in electronic information or an electronic document used in the transaction;
(b) the automated source of information does not give the individual an opportunity to prevent or correct the error;
(c) on becoming aware of the error, the individual promptly notifies the other person; and
(d) in a case where consideration is received as a result of the error, the individual, returns or destroys the consideration in accordance with the other person's instructions, deals with the consideration in a reasonable manner, and does not benefit materially by receiving the consideration.

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

Section VII

19. 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.

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

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

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

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

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

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

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

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

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

Suriname – NONE

Trinidad and Tobago* – LIMITED (GOOD) – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Bill, 2009]

****

18. In the context of contract formation, the fact that a transaction is conducted in electronic form or that information or a record of the negotiation or formation of a contract is in electronic form does not affect its enforceability.

19. Unless parties agree otherwise, an offer or the acceptance of an offer or any other matter that is material to the operation or formation of a contract may be expressed by means of information or a record in electronic form, including by an activity in electronic form such as touching or clicking on an appropriately designated icon or place on the computer screen or otherwise communicating electronically in a manner that is intended to express the offer, acceptance or other matter.

20. A contract may be formed between persons through the interaction of an electronic agent and a person or by the interaction of electronic agents.

Section VII

21. (1) A contract concluded in an electronic environment through the interaction of a person and an electronic agent of another person is voidable where–
    (a) the first referred person made a material error in the information or data message;
    (b) the electronic agent of the second referred person did not provide an opportunity to prevent or correct the error;
    (c) the first referred person notifies the second referred person of the error;
    (d) the second referred person has taken no reasonable steps to correct the error; and
    (e) the first referred person has received or used any material benefit or value from the other person.

(2) Subsection (1) shall not apply to electronic auctions.

22. An electronic data message or record is attributed to a particular person if it resulted from an action of that person or through an agent or electronic agent of that person.

23. Where a person issues an acknowledgement of receipt of an electronic data message or information, that acknowledgement of receipt validates an electronic transaction if, before sending the electronic data message or information or by means of that electronic data message or information, the originator has requested or has agreed with the addressee that receipt of the electronic data message or information be acknowledged.

24. Unless the originator and addressee agree otherwise, information or a data message in electronic form is sent–
    (a) when it enters an information system outside the control of the originator; or
    (b) in the case where the originator and the addressee are in the same information system, when the information or data message becomes capable of being retrieved and processed by the addressee.

25. Unless the originator and addressee agree otherwise, if information or a data message in electronic form is capable of being retrieved by an addressee, it is deemed to be received by the addressee–
    (a) when it enters an information system designated or used by the addressee for the purpose of receiving information or data messages in electronic form of the type sent; or
    (b) upon the addressee becoming aware of the information or data message in the addressee's information system, if the addressee has not designated or does not use an information system for the purpose of receiving information or data message in electronic form of the type sent.

26. Unless the originator and addressee agree otherwise, information or a record in electronic form is deemed to be sent from the originator's address and to be received at the addressee's address.

27. Unless the originator and addressee of a communication agree otherwise, the place of business of either party is deemed to be–
    (a) the place of business that has the closest relationship to the underlying electronic transaction if a party has more than one place of business; or
    (b) if there is no underlying electronic transaction, the principal place of business of the originator or addressee of the communication.

28. If the originator or addressee of a communication has no place of business, then the habitual residence of the originator or addressee is the relevant criterion for the place of sending and receipt of communication.

Section VII

International Best Practices and Regional Trends

1. OECS Model Law

****

Time of Dispatch

6. An electronic communication is taken to be dispatched at the time the electronic communication first enters an information system outside the control of the originator.

Time of Receipt

7. An electronic communications is taken to be received
   (a) in the case of an addressee who has designated an information system for the purpose of receiving electronic communications, at the time the electronic communication enters that information system; or
   (b) in any other case, at the time the electronic communication comes to the attention of the addressee.

Place of Dispatch

8. An electronic communication is taken to be dispatched from-
   (a) the originator's place of business; or
   (b) if the originator has more than 1 place of business,-
      (i) the place of business that has the closest relationship with the underlying transaction; or
      (ii) if there is no place of business to which subparagraph (i) applies, the originator's principal place of business; or
   (c) in the case of an originator who does not have a place of business, the originator's ordinary place of residence.

Place of Receipt

9. An electronic communication is taken to be received at-
   (a) the addressee's place of business; or
   (b) if the addressee has more than 1 place of business,-
      i. the place of business that has the closest relationship with the underlying transaction; or
      ii. if there is no place of business to which subparagraph (i) applies, the addressee's principal place of business; or
   (c) in the case of an addressee who does not have a place of business, the addressee's ordinary place of residence.

2. UNCITRAL Model Law

****

Article 11. Formation and Validity of Contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

Article 12. Recognition by Parties of Data Messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Section VII

(2) The provisions of this article do not apply to the following: [...].

Article 13. Attribution of Data Messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
- (a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
- (b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
- (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
- (b) the data message 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 data messages as its own.

(4) Paragraph (3) does not apply:
- (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
- (b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of Receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by
- (a) any communication by the addressee, automated or otherwise, or
- (b) any conduct of the addressee,

sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:
  (a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
  (b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and Place of Dispatch and Receipt of Data Messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
  (a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
    (i) at the time when the data message enters the designated information system; or
    (ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
  (b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:
  (a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
  (b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...].

Section VII

7.5 Electronic Signatures

International Best Practices and Regional Trends

- The framework identifies what constitutes an electronic signature
- The framework recognizes different classes of electronic signature
- The framework outlines how providers of advanced signature services are to be administered
- Does the framework outline the role, responsibilities and associated liabilities of advanced service providers

Antigua and Barbuda – LIMITED (FAIR) – Comprehensive language utilized to effect policy best practice with regard to advanced e-signatures. Framework requires authorization of certificate service providers by the Minister.

[Electronic Transactions Bill 2006]

****

21. Except as provided in section 22, the provisions of this law shall not be applied so as to exclude, restrict, or deprive of legal effect, any method of creating an electronic signature which -
    (a) satisfies the requirements of section 22 (1); or
    (b) otherwise, meets the requirements of an applicable statutory provision, rule of law, contract.

22. (1) Where the signature of a person is required by a statutory- provision, rule of law or contract, that requirement shall be met in relation to an electronic record if an electronic signature is used that is as reliable and as appropriate for the purpose for which the electronic record was generated or communicated, in all the circumstances, including any relevant agreements.

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

(3) An electronic signature shall be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if -
    (a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;
    (b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;
    (c) any alteration to the electronic signature, made after the time of signing, is detectable; and
    (d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Sub-section (3) does not limit the ability of any person -
    (a) to establish in any other way, for the purpose of satisfying the requirement referred to in sub-section (1), the reliability of an electronic signature; or
    (b) to adduce evidence of the non-reliability of an electronic signature.

23. The Minister may make regulations prescribing methods which satisfy the requirements of Section 22.

Section VII

24. A person relying on an electronic signature shall bear the legal consequences of his failure to -
    (a) take reasonable steps to verify the reliability of an electronic signature; or
    (b) where an electronic signature is supported by a certificate, take reasonable steps to –
        (i) verify the validity, suspension or revocation of the certificate; or
        (ii) observe any limitation with respect to the certificate

25. (1) In determining whether, the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.

(2) If the Minister considers that the practices of a foreign information security service provider provide a level of reliability at least equivalent to that required of information security service providers in order that they may be approved under Part VII, he may by notice published in the Gazette recognize certificates or classes of certificates issued by the foreign provider as legally equivalent to certificates issued by information security service providers approved under Part VII.

(3) The Minister may, by notice published in the Gazette, recognize signatures complying with the laws of a foreign jurisdiction relating to electronic signatures as legally equivalent to signatures issued by information security service providers approved under [relevant law relating to information security service providers] if the laws of the other foreign jurisdiction require a level of reliability at least equivalent to that required for such signatures under this Act.

(4) The Minister may make regulations prescribing the matters to be taken into account by the Minister when deciding whether to exercise his powers under subsections (2) and (3).

(5) Notwithstanding subsections (2) and (3), parties to commercial and other transactions may specify that a particular information security service provider, class of information security service providers or class of certificates shall be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding subsections (2) and (3), the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition in respect of that transaction.

26. (1) The Minister may establish and maintain a register of **approved information security services**, and of providers of such services, which shall contain particulars of every person who, or service which, is for the time being approved under any arrangements in force under section 27.

(2) The Minister may make regulations prescribing the particulars that are to be included in entries in the register maintained under subsection (1).

(3) The Minister shall -
    (a) allow public inspection at all times of an electronic copy of the register; and
    (b) publicize any withdrawal or modification of an approval under section 27, in accordance with arrangements prescribed by the Minister in regulations.

27. The Minister may make regulations enabling the Minister to grant approvals, whether subject to conditions or otherwise, on payment of a prescribed fee, to persons who –
    (a) are providing information security services in Antigua and Barbuda or are proposing to do so; and
    (b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in Antigua and Barbuda or elsewhere.

Section VII

28. (1) References in this part to the provision of an information security service do not include references to the supply of, or of any right to use, computer software or computer hardware unless the supply or the right to use is integral to the provision of information security services which do not consist of such a supply or right to use.

(2) For the purposes of this Part information security services are provided in Antigua and Barbuda if they are provided from premises in Antigua and Barbuda and -

(a) they are provided to a person who is in Antigua and Barbuda when he makes use of the services; or

(b) they are provided to a person who makes use of the services for the purposes of a business carried on in Antigua and Barbuda or from premises in Antigua and Barbuda

29. (1) An information security service provider shall -

(a) act in accordance with the representations it makes with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it –

(i) that are relevant to the certificate throughout its life cycle; or

(ii) which are included in the certificate;

(c) provide reasonably accessible means which enable a person who relies on the certificate to ascertain from the certificate –

(i) the identity of the information security service provider;

(ii) that the person who is identified in the certificate had control of the signature device at the time of signing;

(iii) that the signature device was operational on or before the date when the certificate was issued;

(d) provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise –

(i) the method used to identify the signature device holder;

(ii) any limitation on the purpose or value for which the signature device or the certificate may be used;

(iii) that the signature device is operational and has not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the information security service provider;

(v) whether means exist for the signature device holder to give notice that a signature device has been compromised; and

(vi) whether a timely revocation service is offered;

(e) provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) An information security service provider shall be liable for its failure to satisfy the requirements of subsection (1).

30. The Minister may make regulations prescribing the factors to which regard shall be had in determining whether, and the extent to which, systems, procedures and human resources are trustworthy for the purposes of section 29 (1) (f).

31. The Minister may make regulations prescribing the matters that shall be specified in a certificate.

32. A signature device holder shall -

(a) exercise reasonable care to avoid unauthorized use of its signature device;

(b) without undue delay, notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature if –

(i) the signature device holder knows that the signature device has been compromised; or

(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised; and

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder, which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

The Bahamas – POOR – Very limited consideration of electronic signatures, and the roles of parties in the use of advanced e-signatures

[Electronic Communications and Transactions Act 2003]

****

24.(1) The Minister may make regulations –

(a) for the purpose of establishing how electronic documents may be signed and verified;

(b) respecting the use, import and export of encryption technology, encryption programs, or other encryption products;

(c) for the purpose of authorising, prohibiting or regulating the use of the .bs domain name or any successor domain name for The Bahamas;

Barbados – GOOD (FAIR) – Comprehensive language utilized to effect policy best practice. Limited application of approval process for CSP's is noted.

[Electronic Transactions Act, CAP. 308B]

****

8. (1) Where the law requires the signature of a person, that requirement is met in relation to an electronic record if

(a) a method is used to identify that person and to indicate that person's approval of the information in the electronic record; and

(b) that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) An electronic record that meets the requirements of paragraphs *(a)* and *(b)* of subsection (1) shall not be denied legal effect, validity and enforceability solely on the ground that it is an electronic signature.

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

…

17. An electronic signature that is associated with an accredited certificate issued by an authorized certification service provider under section 18 is deemed to satisfy the requirements of paragraphs *(a)* and *(b)* of section 8(1).

18. (1) The provision of certification services for electronic signatures is not subject to prior authorization by the Minister; but authorization is required for the purposes of section 8.

(2) The Minister, on

(a) the receipt of an application by a certification service provider for the approval of the provision of accredited certificates; and

(b) the payment of such fee as may be prescribed, may, if satisfied that the applicant meets the relevant criteria, by notice published in the *Official Gazette*, authorize the applicant to provide accredited certificates.

Section VII

(3) Subject to subsection (4), the Minister, if satisfied that an authorized certification service provider no longer meets the relevant criteria, may by notice published in the *Official Gazette* revoke an authorization given under subsection (2).

(4) Before revoking an authorization under subsection (3), the Minister shall

(a) give notice in writing to the authorized certification service provider of his intention to do so, indicating his reasons for the proposed revocation; and

(b) invite the authorized certification service provider, within 14 days of the notice, to submit representations in writing as to why the authorization shall not be revoked, and shall consider those representations.

(5) In this section the "relevant criteria" means such policy criteria in respect of electronic signatures or signature products as the Minister may specify by notice published in the *Official Gazette*.

19. (1) The Minister may, by notice published in the *Official Gazette*, recognize certificates or classes of certificates issued in, or certification service providers or classes of certification service providers established in, any other jurisdiction and, upon such recognition and on payment of such fee as may be prescribed

(a) those certificates or classes of certificates shall be deemed to be accredited certificates; and

(b) those certification service providers or classes of certification service providers shall be deemed to be authorized under section 18(2).

(2) In the determination to accord recognition under subsection (1) the Minister shall have regard to whether

(a) the certificates or classes of certificates are required to, and do in fact, meet obligations equivalent to those required for an accredited certificate; and

(b) the certification service providers or classes of certification service providers are required to, and do in fact, meet criteria equivalent to those required for an authorized certification service provider.

(3) The Minister may, by notice published in the *Official Gazette*, revoke any recognition accorded under subsection (1), but, before doing so, the Minister shall

(a) advise the person affected of his intention to do so;

(b) indicate his reasons for the proposed revocation; and

(c) invite that person, within 14 days of the notice, to submit representations in writing as to why the recognition should not be revoked, and shall consider those representations.

20. (1) By issuing an accredited certificate, an authorized certification service provider is liable to any person who reasonably relied on the certificate for

(a) the accuracy of all information in the accredited certificate as from the date on which it was issued, unless the authorized certification service provider has stated otherwise in the accredited certificate;

(b) assurance that the person identified in the accredited certificate held, at the time the accredited certificate was issued, the signature creation device corresponding to the signature verification device given or identified in the accredited certificate;

(c) assurance that the signature creation device and the signature verification device functioned together in a complementary manner, where the service provider generates both devices, unless the person who relied on the accredited certificate knows or ought reasonably to have known that the authorization of the certification service provider has been revoked.

(2) An authorized certification service provider is not liable for errors in the information in an accredited certificate where

(a) the information was provided by or on behalf of the person identified in the accredited certificate; and

(b) the certification service provider can demonstrate that he has taken all reasonably practical measures to verify that information.

(3) An authorized certification service provider that

(a) indicates in the accredited certificate limits on the uses of that certificate; and

(b) makes those limits known to third parties, is not liable for damages arising from the use of the accredited certificate contrary to those limits.

(4) The limits in subsection (3) may include a limit on the value of transactions for which the accredited certificate is valid.

21. (1) The Minister may make regulations

(a) respecting the use, import and export of encryption programmes or other encryption products;

(b) prohibiting the export of encryption programmes or other encryption products from Barbados generally or subject to such restrictions as may be prescribed.

(2) Subject to any regulations made under subsection (1), a person may use any encryption programmes or other encryption product of any bit size or other measure of the strength of the encryption that has lawfully come into the possession of that person.

Belize – NONE

Dominica – NONE

Dominican Republic – GOOD
(INFORMAL TRANSLATION)

Article 31. Attributes of a Signing Digital. The use of a signature Digital shall have the same force and effect as the use of a signature handwritten, if it includes the following attributes;

1 It is unique to the person that uses it;

2. It is likely to be verified;

3 It is under the exclusive control of the person that uses it;

4 Is linked to the information, digital document or message to which you are associated, in such a way that if they are changed, the digital signature is invalidated, and 5 Is in accordance with the regulations adopted by the Executive power.

Article 32. Secure Digital Signature. A secure digital signature is the one that can be verified in accordance with a system of procedure security that complies with the guidelines set by This Act and its regulations.

Article 33. Data Digitally-Signed Messages. Means that a data message has been signed digitally if the symbol or the methodology adopted by the party meets an authentication procedure or Security established by the regulation of this law. When a digital signature has been fixed in a message of data shall be presumed that the Subscriber that had the intention to prove that data message and be linked to the content of the same.

Article 34. Digital Documents Signed Digitally. Means that a digital document has been signed digitally by one or more parties if the symbol or the methodology adopted by each of the parties comply with an established procedure of authentication or security by the regulation of this law. When one or more digital signatures have been laid down in a document Digital, it is presumed that the parties had the intention to prove that digital document and be linked to the content of the same.

Section VII

Article 35. Characteristics and Requirements of the Entities Certification. Without prejudice to this article, may certification bodies be legal persons, both public and private, domestic or overseas, and the Chambers of Commerce and production upon request, be authorized by the Institute Dominican Republic of telecommunications (INDOTEL), and that comply with the requirements laid down in the implementation regulations based on the following conditions:

(a) have the economic and financial capacity sufficient to provide authorized services, such as certification entity;
(b) have the capacity and necessary technical elements for the generation of digital signatures, the issuance of certificates on the authenticity of the same and the conservation of the terms data messages laid down in this law;
(c) without prejudice to the statutory provisions that apply the effect, the legal representatives and Administrators may not be people who have been condemned to deprivation of liberty; or that have been suspended in the exercise of their profession for serious misconduct against the ethics or have been excluded from it. This disqualification is valid for the same period as the indicated by the criminal or administrative law for the purpose, and
(d) the digital signature certificates issued by foreign certification bodies may be recognized in the same terms and conditions of certified by the law for the issuance of certificates by part of the national certification bodies, always and where such certificates are recognized by a entity of authorized certification which guarantees in the same way that makes their own certificates, the regularity of the details of the certificates, as well as its validity and term. In any case, suppliers of certification services are subject to the regulations national responsibility.

Is attribution of the Monetary Board, within its privileges, regulate all with regard to the operations and financial services associated with the means of payment e to carry out the national financial system, and corresponds to the supervision of the same to the Superintendency of banks, under the provisions of legislation banking force.

Article 36. Activities of Certification Authorities. Certification entities authorized by the Institute Dominican Republic of telecommunications (INDOTEL) in the country, they may provide the following services, without prejudice of the regulatory power of the regulatory body for modify the following list:

(a) issue certificates in connection with digital signatures persons or legal entities;
(b) provide or facilitate the creation of signatures services Certified digital;
(c) offer or facilitate registration services and time stamp in the transmission and reception of data;
(d) issuing certificates in relation to the person possessing a right concerning the documents listed in the numerals 6 and 7 of article 27 of this Act.

Article 37. Audit Certification Institutions. The Dominican telecommunications Institute (INDOTEL) retains the same right to inspection granted by the law-General of telecommunications, No.153-98, of 27 of May 1998, and in the case of explicit modification of that text, the present article shall be construed so is in accordance with the legislation of telecommunications.

Article 38. Manifestation of the Practice of the Entity's Certification. Each authorized certification authority shall publish, in a repository of the Dominican Institute of the Telecommunications (INDOTEL) or in the repository to the regulatory body designated by a practical demonstration of entity certificate containing the following information:

(a) the name, address and telephone number of the entity certification;
(b) the current public key of the certification body;
(c) the outcome of the evaluation obtained by the entity's certification in the most recent audit carried out by the Instituto Dominicano de las Telecomunicaciones (INDOTEL);

(d) if the authorization to operate as an entity of certification has been revoked or suspended. In both cases is revoked or suspended the public key of the certification entity. This register shall include also the date of the revocation or suspension for operate;
(e) the limits imposed on the certification entity in the authorization to operate;
(f) any event which substantially affects the ability to the certification entity to operate;
(g) any information required by rules of procedure.

Article 39. Remuneration for the Provision of Services. The remuneration for the services of the entities of certification shall be freely established by them, to less than the Dominican Institute of telecommunications (INDOTEL), reasoned decision, determined that, in a particular case, do not exist in the market of services the sufficient conditions to ensure competition effective and sustainable.

Article 40. Obligations of the Certification Bodies. Certification bodies will have, among other things, the following obligations:
(a) issue certificates in accordance with the requested or agreed by the Subscriber;
(b) implement the systems of security to ensure the issuance and creation of digital signatures;
(c) ensure the protection, confidentiality and proper use the information provided by the Subscriber;
(d) ensure the permanent provision of services of certification entity;
(e) respond in a timely manner the requests and complaints made by subscribers;
(f) carry out the notices and publications in accordance with the established in this Act and its regulations;
(g) provide the information that require you the judicial or competent administrative bodies in relationship with digital signatures and certificates issued and, in general, on any message data is find under their custody, and management;
(h) update its technical elements for the generation of digital signatures, the issuance of certificates on the authenticity of them, preservation and archiving of supported data messages and all other documents authorized, subject to the necessary regulations service to ensure protection to consumers of their services;
(i) facilitate the conduct of audits by the Instituto Dominicano de las Telecomunicaciones (INDOTEL);
(j) published in a repository of audit practice for certification, subject to the terms and conditions arranged in the regulations.

Article 41. Unilateral Termination. Unless agreed between the parties, the entity for certification You may terminate the relationship agreement with the Subscriber, giving notice of not less than ninety within (90) days. Expiry of this term, the entity's certification shall revoke the certificates that are pending expiry. Also, the Subscriber may to terminate the agreement in connection with the entity certification giving notice of not less to thirty (30) days.

Article 42. Liability of the Certification Authority. Unless agreed between the parties, entities of certification will respond for the damages that cause to anyone.

Article 43. Cessation of Activities by Entities Certification. Authorized certification authorities may cease in the exercise of their activities, prior notification to the Instituto Dominicano de las Telecomunicaciones (INDOTEL), within a period not less than ninety (90) days prior to the cessation of activities by the certification entity, without prejudice to the Faculty of the regulator of regulate what is necessary to preserve the protection to the consumers of their services. In the implementation of this Article, and where necessary their interpretation, be taken into account that there is an obligation of ensure the protection, confidentiality and proper use of the information provided by the Subscriber.

Section VII

Grenada* – LIMITED (FAIR) – Provisions regarding e-signatures and advanced e-signatures according to best practice. However there seems confusion over the role of the Certifying Authority as either a Service Provider or oversight body.
[Electronic Transactions Bill, 2008]
****

29. (1) In this Part, "relying party" means a person who may act of relying on the basis of a certificate or encrypted signature.

(2) A relying party shall bear the legal consequences of that party's failure
- (a) to take reasonable steps to verify the reliability of an encrypted signature;
- (b) where an encrypted signature is supported by a certificate, to take reasonable steps to verify the validity and currency of the certificate and to observe any limitation with respect to the certificate.

30. A signatory who has an encrypted signature creation device shall
- (a) exercise reasonable care to avoid unauthorized use of that device;
- (b) forthwith notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of, the signature, if the signatory knows
  - (i) that the device has been compromised; or
  - (ii) of circumstances which give rise to a substantial risk that the device may have been compromised;
- (c) where a certificate is used to support an encrypted signature, exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by the signatory in or in relation to the certificate;
- (d) indicate, in any document to which he affixes his encrypted signature, whether he does so in a personal capacity or an official capacity.

31. (1) A certification service provider who issues a certificate shall
- (a) act in accordance with the representations made by it service provider. with respect to its policies and practices;
- (b) exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by it in relation to the certificate;
- (c) provide reasonably accessible means for enabling a relying party to ascertain from the certificate-
  - (i) the identity of the certification service provider;
  - (ii) that the signatory identified in the certificate had control of the encrypted signature creation device at the time when the certificate was issued; and
  - (iii) that the encrypted signature creation device was valid at the time when the certificate was issued;
- (d) provide reasonably accessible means for enabling a relying party to ascertain from the certificate or otherwise
  - (i) the method used to identify the signatory;
  - (ii) every limitation on the purpose or value for which the encrypted signature creation device or the certificate may be used;
  - (iii) whether the encrypted signature creation device is valid and has not been comprised;
  - (iv) every limitation on the scope or extent of liability stipulated by the certification service provider;
  - (v) the facilities provided for the signatory to give notice pursuant to section 30(b);
  - (vi) the procedures in place to effect revocation;
- (e) provide a means for a signatory to give notice pursuant to section 30(b);
- (f) ensure the availability of a timely revocation service;
- (g) utilize trustworthy systems, procedures and human resources in performing its services.

Section VII

(2) For the purposes of this section, in determining whether any systems, procedures or human resources utilized by a certification service provider are trustworthy, regard may be had to
- (a) the provider's financial and human resources, including the existence of assets and the quality of his hardware and software systems;
- (b) the provider's procedures for processing certificates and applications for certificates;
- (c) the provider's retention of records and the availability of information to relying parties and to signatories identified in certificates;
- (d) the regularity and extent of audits of the provider's operations by an independent body;
- (e) any other relevant factor.

33. (1) In determining whether or to what extent an electronic of foreign document is legally effective, no regard shall be had to the location where the information was created or used, or the originator's place of business.

(2) An electronic signature created or used outside Grenada shall have the same legal effect in Grenada as an electronic signature created or used in Grenada if it offers a substantially equivalent level of reliability.

(3) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of subsection (2), regard shall be had to recognized international standards and to any other relevant factors.

…..

42. (1) For the purposes of this Act there shall be a Certifying Authority, which shall have the functions specified in subsection (2).

(2) The Certifying authority shall be the [Trade Board] or such other person as the Minister may designate by notice published in the Gazette.

(3) The functions of the Certifying Authority shall be to
- (a) issue certificates;
- (b) issue and regulate the use of private and public key pairs;
- (c) authorize and regulate the issue of certificates by certification service providers;
- (d) authenticate certificates issued by any local or overseas certification service provider;
- (e) provide time stamping services in relation to electronic documents;
- (f) provide application programming interface, including data encryption, encrypted signatures and digital envelopes;
- (g) carry out any other duties assigned to it under this or any other enactment.

(4) For the purpose of exercising its functions under this section, the Certifying Authority may
- (a) carry out such investigations as may be necessary;
- (b) co-operate with any overseas certifying authority in establishing a system of mutual certification;
- (c) issue certification practice statements from time to time;
- (d) with the approval of the Minister, make regulations prescribing
  - (i) the fees to be imposed for the issue of certificates, authorizations to certification service providers and private and public key pairs;
  - (ii) the manner of application and the requirements for authorization of certification service providers;
  - (iii) standards and codes of conduct for intermediaries and certification service providers.

Guyana – NONE

Haiti – NONE

Section VII

Jamaica – GOOD
[Electronic Transactions, 2006]
****

8. (1) A law requiring a person's signature in relation to any information shall be taken to have been met where the information is given electronically and –
(a) a method is used to identify the person and to show the person's approval of the information given;
(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 information was communicated;
(c) if the signature is required to be given to the Government and the Government requires that the method used be in accordance with particular technology requirement, the Government requirement has been met; and
(d) if the signature is required to be given to a person other than the Government, that person consents to that requirement being met by using the method mentioned in paragraph (a).

(2) Subject to subsection (3), an encrypted 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 by identifying that person;
(c) created by using means that such person can maintain under his sole control; and
(d) linked to the information to which it relates in such a manner that any subsequent alteration of the information 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 an encrypted signature or other method of indicating identity and approval;
(b) adduce evidence of the unreliability of an encrypted signature

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

(5) In determining whether, or to what extent, a certificate or an encrypted signature is legally effective, no regard shall be has to the geographic location –
(a) where the certificate is issued or the encrypted signature is created or used; or
(b) of the place of business of the certificate service provider or signatory.

(6) This section shall not affect the operation of any other law that requires –
(a) information that is given electronically to contain an encrypted signature (however described)
(b) information that is given electronically to contain a unique identification in an electronic form; or
(c) a particular method to be used for information that is given electronically to identify the originator and to show that the originator approved the information given.

…

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (FAIR) – The approach adopted provides no distinction between electronic signatures and advanced electronic signatures. Also there is no consideration of the establishment of oversight of the service provider marketplace in the jurisdiction.

[Electronic Transactions Bill, 2007]

****

20. Unless otherwise provided by a law in force in St. Lucia, parties to a transaction may agree to the use of a particular method or form of electronic signature.

21. (1) Subjection to subsection (2), a legal requirement for a signature other than the signature of a witness is satisfied by means of an electronic signature if the electronic signature –

(a) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and

(b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

(2) A legal requirement for a signature is not satisfied by means of an electronic signature unless, in the case of as signature on information that is required to be given to a person, that person consents to receiving the electronic signature.

…

23. (1) For the purposes of sections 21 and 22, it is presumed that an electronic signature is as reliable as is appropriate where –

(a) the means of creating the electronic signature is linked to the signatory and to no other person

(b) the means of creating the electronic signature was under the control of the signatory and no other person

(c) if any alteration to the electronic signature made after the time if signing is detectable; and

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

(2) Subsection (1) does not prevent any person from proving other grounds or by other means that an electronic signature –

(a) is as reliable as is appropriate; or

(b) is not as reliable as is appropriate.

Saint Vincent and the Grenadines – GOOD – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Act, 2007]

****

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

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

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

Section VII

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

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

(a) the signature creation data is linked to the signatory and no other person;
(b) the signature creation data at the time of signing is under the control of the signatory and no other person;
(c) any alteration to the electronic signature, made after the time of signing is detectable; and
(d) where a purpose of the legal requirement for a signature is to provide assurance as to the soundness of the information to which it relates, any alteration made to that information after the time of signing is detectable.

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

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

23. The Minister may make Regulations prescribing methods which satisfy the requirements of section 22.

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

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

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

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

28. (1) The Accreditation Authority may -

(a) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this Act;
(b) temporarily suspend or revoke the accreditation of an authentication product or service; and
(c) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this Act.

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

(a) authentication products or services accredited in terms of section 30;
(b) authentication products and services recognized in terms of section 32;
(c) revoked accreditations or recognitions; and
(d) any other information as may be prescribed.

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

Section VII

(2) An application for accreditation shall -
(a) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and
(b) accompanied by a non-refundable prescribed fee.

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

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

…

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

(2) The following particulars in respect of a cryptography provider shall be recorded in the register:
(a) the name and address of the cryptography provider;
(b) a description of the type of cryptography service or product being provided; and
(c) any other particulars as may be prescribed to adequately identify and locate the cryptography provider and its products or services.

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

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

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

(3) For the purposes of subsection (1), a cryptography service or product is regarded as being provided in the State if it is provided:
(a) from premises in the State;
(b) to a person who is present in the State when that person makes use of the service or product; or
(c) to a person who uses the service or product for the purposes of a business carried on in the State or from premises in the State.

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

(2) Subsection (1) shall not apply in respect of information which is disclosed:
(a) to a relevant authority which investigates a criminal offence or for the purposes of criminal proceedings;
(b) to government agencies responsible for safety and security in the State pursuant to an official request;
(c) to a cyber inspector;
(d) pursuant to the provisions of the Freedom of Information Act 2003; or
(e) for the purposes of any civil proceedings which relate to the provision of cryptography services or products and to which a cryptography provider is a party.

Section VII

Suriname – NONE

Trinidad and Tobago – LIMITED (FAIR) – Provisions relating to e-signatures and advanced e-signatures according to best practice. However there is a limited framework for the authorization of CSP's.

[Electronic Transactions Bill, 2009]

****

29. Parties to an electronic transaction may agree to the use of a particular method or form of electronic signature, unless otherwise provided by written law.

30. Where a written law requires the signature of a person, that requirement is met in relation to an electronic record or data message by the use of an electronic signature that meets the minimum standards of reliability and integrity or is as reliable as appropriate, given the purpose for which and the circumstances in which the signature is required.

31. The criteria that shall be used to determine the reliability and integrity of an electronic signature include whether–

(a) the authentication technology uniquely links the user to the signature;

(b) it is capable of identifying the user;

(c) the signature is created using a means that can be maintained under the sole control of the user; and

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

32. The Minister may make regulations setting out a particular form of electronic signature to meet a specific legal requirement.

33. An electronic signature that is associated with a certificate issued by a certification service provider registered under Part V, (hereinafter referred to as an "accredited certificate") is deemed to satisfy the requirements set out in section 31 for reliability and integrity.

34. No person shall issue accredited certificates to the public unless he is registered with the Data Commissioner as a certification service provider and has provided the information required by the Minister by Order.

35. (1) Subject to section 43, a person wishing to be registered as a certification service provider in order to issue accredited certificates to the public, shall apply to the Data Commissioner in the manner prescribed and pay the prescribed fee.

(2) The application under subsection (1) shall include at a minimum a statement of compliance with the requirements set out in section 36.

…

36. A certification service provider that issues accredited certificates to the public shall conduct his or its operations in a reliable manner and shall–

(a) employ personnel who possess the expert knowledge and experience required for these operations, especially with regard to management, technology and security procedures;

(b) apply such administrative and management routines that conform to recognized standards;

(c) use trustworthy systems and products that are protected against modification and that ensure technical and cryptographic security;

(d) maintain sufficient financial resources to conduct his or its operations in accordance with these requirements and any other provisions set forth in the Act and bear the risk of liability for damages;

Section VII

(e) have secure routines to verify the identity of those signatories to whom accredited certificates are issued;
(f) maintain a prompt and secure system for registration and immediate revocation of accredited certificates;
(g) take measures against forgery of accredited certificates and, where applicable, guarantee full confidentiality during the process of generating signature creation data;
(h) comply with section 57; and
(i) comply with any other requirements established by the Minister by Order.

37. The Data Commissioner shall maintain a public registry of certification service providers that includes the information required by the Minister by Order.

38. A registered certification service provider that issues accredited certificates shall annually provide the Data Commissioner with an updated notification of compliance with the requirements of section 36 and pay the prescribed fee.

39. (1) The Data Commissioner may conduct an audit to verify that the certification service provider has been or remains in compliance with the requirements of this Act.

(2) In the performance of an audit, the Data Commissioner may employ whatever experts he considers may be required.

…

42. Where the Data Commissioner is satisfied that a certification service provider no longer meets the requirements to issue accredited certificates, he may–
(a) cancel the registration of the certification service provider;
(b) order the certification service provider to cease any or all of its activities, including the provision of accredited certificates;
(c) order the certification service provider to be removed from the registry;
(d) take any action that he deems reasonable to ensure that the certification service provider is in compliance with the requirements set out in section 36; or
(e) make any other order that the Data Commissioner deems reasonable in the circumstances including, but not limited to reimbursement of fees and charges to users of the certification service providers services or public notification of cessation of business.

43. (1) The Minister may by Order recognize certificates or classes of certificates as accredited certificates issued by certification service providers or classes of certification service providers established in any other jurisdiction, as accredited certificates.

(2) Where the Minister makes an Order under subsection (1) the certification service providers named in the Order shall be deemed to be registered for the purposes of this Part and the Data Commissioner shall enter the names of such service providers in accordance with section 37.

International Best Practices and Regional Trends

1. OECS Model Law

Requirement for Signature

18 (1) Subject to subsection (2), a legal requirement for a signature other than a witness' signature is met by means of an electronic signature if the electronic signature –
(a) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and

(b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

(2) A legal requirement for a signature is not met by means of an electronic signature unless, in the case of a signature on information that is required to be given to a person, that person consents to receiving the electronic signature.

Requirement that Signature or Seal be Witnessed

19.(1) Subject to subsection (2), a legal requirement for a signature or a seal to be witnessed is met by means of a witness' electronic signature, if-

(a) in the case of the witnessing of a signature, the signature is an electronic signature that complies with section 18; and

(b) in the case of the witnessing of a signature or a seal, the electronic signature of the witness–

i. adequately identifies the witness and adequately

ii. indicates that the signature or seal has been witnessed; and

(c) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness' signature is required.

(2) A legal requirement for a signature or seal to be witnessed is not met by means of a witness' electronic signature unless, in the case of a witness' signature on information that is required to be given to a person, that person consents to receiving the witness' electronic signature.

Presumption About Reliability of Electronic Signatures

20.(1) For the purposes of section 18 and 19, it is presumed that an electronic signature is as reliable as is appropriate if –

(a) the means of creating the electronic signature is linked to the signatory and to no other person; and

(b) the means of creating the electronic signature was under the control of the signatory and of no other person; and

(c) any alteration to the electronic signature made after the time of signing is detectable; and

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

(2) Subsection (1) does not prevent any person from proving on other grounds or by other means that an electronic signature-

(a) is as reliable as is appropriate; or

(b) is not as reliable as is appropriate.

2. EU Directive 1999/ 93/ EC (e-Signatures)

Article 3

Market Access

1. Member States shall not make the provision of certification services subject to prior authorization.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognized by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

Article 4

Internal Market Principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal Effects of Electronic Signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
   (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
   (b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
   – in electronic form, or
   – not based upon a qualified certificate, or
   – not based upon a qualified certificate issued by an accredited certification-service-provider, or
   – not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

7.6 Consumer Protection

International Best Practices and Regional Trends

- The framework provides for the voidance of electronic contracts
- The framework provides specific requirements of the vendor in the execution of electronic contracts with consumers
- The framework provides protection of the consumer from unwarranted communications

Antigua and Barbuda – LIMITED (FAIR) – Adequate provisions covering the disclosure of information by vendor, but there is no consideration provided for opportunity for verification by consumer, nor for treatment of unsolicited commercial messages
[Electronic Transactions Bill 2006]
****

42. (1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow:
(a(the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number;
(b) prompt, easy and effective consumer communication with the seller;
(c) service of legal process.

(2) A person using electronic communications to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate records of the information.

(3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction, and notably:
(a) terms, conditions and methods of payment; and
(b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

The Bahamas – NONE

Barbados – NONE

Belize – GOOD – Adequate provisions covering the disclosure of information by vendor, but there is no consideration for treatment of unsolicited commercial messages. The connection with clause 20 could be more explicit

Section VII

[Electronic Transactions Act, 2003 Chap 290:01]
****

20. (1) An electronic transaction between an individual and another person's automated source of information has no legal effect if :
(b) the automated source of information does not give the individual an opportunity to prevent or correct the error;

24. (1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow:
(a) the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number;
(b) prompt, easy and effective consumer communication with the seller; and
(c) service of legal process.

(2) A person using electronic communications to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information.

(3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction, and notably:
(a) terms, conditions and methods of payment; and
(b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

Dominica – FAIR

Dominican Republic – NONE

Grenada* – LIMITED (GOOD) – Comprehensive provisions in line with best practices
[Electronic Transactions Bill, 2008]
****

35. (1) This Part applies only to the formation, by means of electronic transactions, of agreements for the supply of goods, services or facilities, for the sale, hire or exchange, and to the performance of such agreements.

(2) This Part applies to any supplier who
(a) in Grenada, offers goods, services or facilities for sale, hire or exchange, to any person in Grenada; or
(b) whether in or outside of Grenada, offers goods, services or facilities, for sale, hire or exchange, to any person in Grenada.

36. (1) A supplier shall, on the website where goods, services or facilities of supplier are offered for sale, hire or exchange by the supplier, make available to in conduct of the consumer, the information set out in the Second Schedule.

(2) The supplier shall provide the consumer with an opportunity to do the following , in the following order of sequence transactions.
(a) review the entire electronic transaction;
(b) correct any errors;
(c) withdraw from the transaction before finally placing an order; and
(d) access electronically and reproduce an accurate summary of the order and the terms, including the total cost relating thereto.

Section VII

(3) Where a supplier fails to comply with subsection (1) or (2), the consumer is entitled to cancel the transaction within fourteen days after receiving the goods, services or facilities to which the transaction applies.

(4) Where a transaction is cancelled under subsection (3)
- (a) the consumer shall return the goods and cease using the services or facilities supplied pursuant to the transaction, as the case may require;
- (b) the supplier shall refund all payments made by the consumer in respect of the transaction.

(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).

37. (1) Subject to subsections (2) and (4), a consumer is entitled to cancel, without giving any reason and without incurring any charge or penalty, any transaction or credit agreement for the supply of
- (a) goods, within seven days after the receipt of the goods; or
- (b) services or facilities, within seven days after the date on which the agreement is made.

(2) This section does not apply to any transaction
- (a) for financial services, including investment services, insurance and reinsurance operations and banking services;
- (b) conducted at 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) are of such a nature that they cannot be returned;
  - (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.

(3) Subject to subsection (4), if payment for the goods, services or facilities, as the case may be, is made prior to a cancellation under subsection (1), the consumer is entitled to a full refund of the payment, and the supplier shall make the refund with thirty days after the date of cancellation.

(4) The only charge that may be levied on a consumer who acts under subsection (1) is the direct cost to the supplier of returning the goods.

(5) Nothing in this section shall be construed to prejudice any other rights that the consumer may have under any other law.

Section VII

38. (1) A person who sends unsolicited commercial communications to consumers shall give to a consumer to whom any such communication is sent
(a) the opportunity to decline to receive any further such communications from that person; and
(c) upon request by the consumer, the identifying particulars of the source from which that person obtained the consumer's contact information or other personal information.

(2)A person who fails to comply with subsection (1) commits an offence.

(3) No agreement is concluded where a consumer fails to respond to an unsolicited commercial communication.

(4) A person commits an offence if that person sends an unsolicited commercial communication to a consumer who has communicated to that person that the consumer does not wish to receive any such communication.

39. (1) Where an agreement is made for the supply of goods, services or goods, facilities, the supplier shall supply the goods, services or facilities, as the case may require, within the time specified in the agreement or, if no time is specified, within thirty days after the date on which the agreement is made.

(2) If the supplier fails to supply the goods , services or facilities, as the case may require, within the time required under subsection (1), the consumer may cancel the agreement seven days after giving notice to the supplier of that intention .

(3)Where the supplier is unable to carry out the agreement because the goods, services or facilities are unavailable, the supplier shall
(a) forthwith notify the consumer of the inability; and
(b) within thirty days after becoming aware of the inability, refund any payment made by, or on behalf of, the consumer in respect of the goods, services or facilities.

40. No provision in any agreement shall be construed as excluding any rights or obligations provided for in this Part.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD – Comprehensive provisions in line with best practices. "Cooling off" provisions unique (with St. Vincent and the Grenadines) inclusion into this framework.
[Electronic Transactions, 2006]
****

27. (1) A supplier shall, on the website where goods, services or facilities are offered for sale, hire or exchange by the supplier, make available to the consumer the information set out in the Second Schedule.

(2) The supplier shall provide the consumer with an opportunity to do the following, in the order of their occurrence herein –
(a) review the entire electronic transaction;
(b) correct any errors;
(c) withdraw from the transaction before finally placing an order; and
(d) access electronically and reproduce an accurate summary of the order and the terms, including the total cost, relating thereto.

(3) Where a supplier fails to comply with subsection (1) or (2), the consumer is entitled to cancel the transaction within fourteen days after receiving the goods, services or facilities to which the transaction applies.

(4) Where a transaction is cancelled under subsection (3) –
- (a) the consumer shall return the goods and cease using the services or facilities pursuant to the transaction, as the case may require;
- (b) the supplier shall refund all payments made by the consumer in respect of the transaction.

(5) The supplier shall utilize a payment system that is sufficiently secure having regard to –
- (a) accepted technological standards at the time of the transaction; and
- (b) 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).

28. (1) Subject to subsections (2) and (4), a consumer is entitles to cancel, without giving any reason and without incurring any charge or penalty, any transaction or credit agreement for the supply of –
- (a) goods, within seven days after the receipt of the goods; or
- (b) services or facilities, within seven days after the date on which the agreement is made.

(2) This section does not apply to any 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.

(3) Subject to subsection (4), if payment for the goods, services or facilities, as the case may be, has been made prior to a cancellation under subsection (1), the consumer is entitles to a full refund of the payment, and the supplier shall make the refund within thirty days after the date of the cancellation.

(4) The only charge that may be levied on a consumer who acts under subsection (1) is the direct cost to the supplier of returning the goods.

(5) Nothing in this section shall be construed to prejudice any other rights that the consumer may have under any other law.

Section VII

29. (1) A person who sends unsolicited commercial communications to consumers shall give to a consumer to whom any such communication is sent –
(a) the opportunity to decline to receive any further such communications from that person; and
(b) upon request by the consumer, the identifying particulars of the source from which that person obtained the consumer's contact information or other personal information.

(2) A person who fails to comply with subsection (1) commits an offence.

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (GOOD)
[Electronic Transactions Bill, 2007]
****

40 (1) Subject to subsection (2) and unless otherwise agreed by parties who are not consumers, and without prejudice to any consumer rights under the provision of any other law in force in Saint Lucia, the originator shall provide information in clear, comprehensive and unambiguous terms regarding the matters set out In Regulations.

(2) Information pursuant to subsection (1) shall be provided to the addressee, prior to the placement of the order by the addressee.

(3) Unless parties who are not consumers have agreed otherwise, an originator shall indicate which relevant codes of conduct the originator subscribed to and provide information as to how these codes may be accessed electronically

(4) Where the originator provides terms and conditions applicable to the addressee contract to the addressee, the originator shall make them available to the address in a way that allows the addressee to store and reproduce them.

(5) subsection (1) and (2) shall not apply to contracts concluded by exchange of electronic mail or by equivalent individual communications.

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

42. (1) An electronic transaction between an individual and another person's automated source of information has no legal effect if –
(a) the individual makes a material error in electronic information or an electronic document used in the transaction;
(b) the automated source of information does not give the individual an opportunity to prevent or correct the error;
(c) on becoming aware of the error, the individual promptly notifies the other person; and
(d) in a case where consideration is received as a result of the error, the individual, returns or destroys the consideration in accordance with the other person's instructions or, if there are no instruction, deals with the consideration is a reasonable manner and does not benefit materially by receiving the consideration

(2) This section does not limit the operation of any other law in force in Saint Lucia relating to mistake.

Section VII

Saint Vincent and the Grenadines – GOOD – Comprehensive provisions in line with best practices. Provisions for "cooling off" period is unique (with Jamaica) among frameworks reviewed

[Electronic Transactions Act, 2007]

****

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

(a) its full name and legal status;
(b) its physical address and telephone number;
(c) its web site address and e-mail address;
(d) the physical address where the supplier will receive legal service of 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 manner of payment;
(h) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
(I) the time within which the goods will be dispatched or delivered or within which the services will be rendered;
(j) the manner and period within which consumers can access and maintain a full record of the transaction;
(k) the return, exchange and refund policy of the supplier;
(l) the security procedures and privacy policy of the supplier in respect of payment, payment information and personal information; and
(m) the rights of consumers under section 36, where applicable.

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

(a) to review the entire electronic transaction;
(b) to correct any mistakes; and
(c) to withdraw from the transaction before finally placing any order.

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

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

(a) of goods within 7 days after the date of receipt of the goods; or
(b) of services within 7 days after the date of conclusion of the agreement.

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

Suriname – NONE

Trinidad and Tobago – LIMITED (GOOD) – Comprehensive provisions in line with best practices. The connection with Clause 21 could be more explicit.
[Electronic Transactions Bill, 2009]
****

21. (1) A contract concluded in an electronic environment through the interaction of a person and an electronic agent of another person is voidable where–

(b) the electronic agent of the second referred person did not provide an opportunity to prevent or correct the error;

(2) Subsection (1) shall not apply to electronic auctions.

….

56. (1) Suppliers with a place of business in Trinidad and Tobago who knowingly use an intermediary or a telecommunications service provider based in Trinidad and Tobago for effecting an electronic transaction shall, before the conclusion of the electronic contract based on such transaction, provide certain information to consumers in respect of such electronic contract.

(2) The information shall include but not be limited to–

(a) the identity, address and telephone number of the supplier;
(b) a detailed description of the characteristics of the goods or services including any system or technical requirements;
(c) the amount to be paid including taxes, the currency in which the amount must be paid, the method of payment and the security arrangement for performance;
(d) the cancellation, refund or exchange policy;
(e) the expected date of delivery, where applicable;
(f) the privacy policy;
(g) a copy of the contract for the consumer in a format that can be retained;
(h) the arrangements for payment, delivery or performance; and
(i) the existence of a right of withdrawal.

(3) This section shall not apply to contracts concluded at an electronic auction.

57. A consumer who is not provided with the information required by section 56 has the right to rescind the contract within thirty calendar days provided that the consumer has not received any material benefit from the transaction.

58. Before entering into a contract requiring the issuance of an accredited certificate, a certification service provider shall inform the party seeking the certificate in writing of the following:

(a) the terms and conditions concerning the use of the certificate, including any limitations on its scope or amounts;

Section VII

(b) any requirements concerning storage and protection of the signature-creation data by the signatory;
(c) the cost of obtaining and using the certificate and of using the other services of the certification authority;
(d) whether the certification authority is accredited under a voluntary accreditation scheme or by an accreditation body in another jurisdiction; and
(e) procedures for settlement of complaints.

59. Any person who sends unsolicited commercial communications through electronic media to consumers based in Trinidad and Tobago or knowingly uses an intermediary or a telecommunications service provider based in Trinidad and Tobago to send, or who has a place of business in Trinidad and Tobago and sends, unsolicited electronic correspondence to consumers shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

International Best Practice and Regional Trends

European Union

Directive 2000/ 31/EC

Article 6 – Information to be Provided

In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:
(a) the commercial communication shall be clearly identifiable as such;
(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7 – Unsolicited Commercial Communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Section VII

7.7 Intermediaries and Telecommunications Service Providers

International Best Practices and Regional Trends

- The framework specifies persons that can be identified as intermediaries
- The framework outlines responsibilities of intermediaries and telecommunications providers in the facilitation of an electronic contract, or transmittal of an electronic document
- The framework outlines limitations to the liabilities of these persons in the instance that there is illegal activity associated with an electronic document or contract that has been facilitated by the provider

Antigua and Barbuda – LIMITED (GOOD) – Comprehensive provisions in accordance with best practice.

[Electronic Transactions Bill 2006]

****

35. (1) the intermediary or service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of electronic records via an information system under its control, as long as the intermediary or service provider–
    (a) does not initiate the transmission;
    (b) does not select the addressee;
    (c) performs the functions in an automatic, technical manner without selection 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.

36. An intermediary or service provider that transmits an electronic record provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that electronic record, where the purpose of storing such electronic record is to make the onward transmission of the electronic record more efficient to other recipients of the service upon their request, as long as the service provider–
    (a) does not modify the electronic record;
    (b) complies with conditions on access to the electronic record;
    (c) complies with rules regarding the updating of the electronic record, specified in a manner widely recognized and used by industry;
    (d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain information on the use of the electronic record; and
    (e) removes or disables access to the electronic record it has stored upon receiving a take-down notice referred to in section 39.

37. (1) An intermediary or service provider that provides a service that consists of the storage of electronic records provided by a recipient of the service, is not liable for damages arising from information stored at the request of the recipient of the service, as long as the service provider–

Section VII

(a) does not have actual knowledge that the information or an activity relating to the information is infringing the rights of a third party; or
(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the information is apparent; and
(c) upon receipt of a take-down notification referred to in section 39, acts expeditiously to remove or to disable access to the information.

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

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

38. An intermediary or service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing electronic record or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the intermediary or service provider–
(a) does not have actual knowledge that the electronic record or an activity relating to the electronic record is infringing the rights of that person;
(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic record is apparent;
(c) does not receive a financial benefit directly attributable to the infringing activity; and
(d) removes, or disables access to, the reference or link to the electronic record or activity within a reasonable time after being informed that the electronic record or the activity relating to such electronic record, infringes the rights of a person.

39. (1) For the purposes of this Part, a notification of unlawful activity must be in writing, must be addressed by the complainant to the intermediary or service provider or its designated agent and must include–
(a) the full names and address of the complainant;
(b) the written or electronic signature of the complainant;
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the intermediary or service provider in respect of the complaint;
(f) telephonic and electronic contact details, if any, of the complainant;
(g) a statement that the complainant is acting in good faith;
(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and

(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts commits an offence and is liable for damages for wrongful takedown.

(3) An intermediary or service provider is not liable for wrongful takedown in response to a notification.

40. (1) An intermediary or service provider shall not be required to monitor any electronic record processed by means of his system in order to ascertain whether its processing would (apart from this section) constitute or give rise to an offence or give rise to civil liability.

(2) Except as provided by subsection (1), nothing in this section shall relieve an intermediary or service provider from -

(a) any obligation to comply with an order or direction of a court or other competent authority; or
(b) any contractual obligation.

The Bahamas – GOOD – Comprehensive provisions in accordance with best practice.
[Electronic Communications and Transactions Act 2003]
****

19. (1) An intermediary shall not be subject to any civil or criminal liability in respect of third-party information contained in an electronic communication for which such intermediary is only providing access and he –
(a) has no actual knowledge that the information gives rise to civil or criminal liability;
(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or
(c) follows the procedure set out in section 20 if the intermediary -
(i) acquires knowledge that the information gives rise to civil or criminal liability; or
(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary shall not be required to monitor any information contained in an electronic communication in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

(3) Nothing in this section shall relieve an intermediary from complying with any court order, injunction, writ, Ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic communication.

(4) For the purposes of this section -

"provides access", in relation to third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing access;

"third-party information" means information of which the intermediary is not the originator.

20. (1) If an intermediary has actual knowledge that the information in an electronic communication gives rise to civil or criminal liability, as soon as practicable thereafter the intermediary shall -
(a) remove the information from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information; and
(b) notify the police of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary.

(2) If an intermediary is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic communication ought reasonably to have been known, as soon as practicable thereafter the intermediary shall –
(a) follow the relevant procedure set out in any code of conduct that is applicable to such intermediary under section 21; or
(b) notify the police and the Minister.

(3) Upon being notified in respect of any information under subsection (2), the Minister may direct the intermediary to -

(a) remove the electronic communication from any information processing system within the control of the intermediary; and

(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication.

(4) An intermediary shall not be liable, whether in contract, tort, under statute or pursuant to any other right, to any person, including any person on whose behalf the intermediary provides services in respect of information in an electronic communication, for any action the intermediary takes in good faith in exercise of the powers conferred by, or as directed by the Minister under, this section.

Barbados – GOOD – Comprehensive language utilized to effect policy best practice.

[Electronic Transactions Act, CAP. 308B]

****

23. (1) An intermediary is not subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services where the intermediary

(a) was not the originator of that electronic record;

(b) has no actual knowledge that the information gives rise to civil or criminal liability;

(c) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or

(d) follows the procedure set out in section 24, if the intermediary

(i) acquires knowledge that the information gives rise to civil or criminal liability, or

(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

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

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

24. (1) Where an intermediary has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, or is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic record ought reasonably to have been known, as soon as practicable the intermediary shall

(a) remove the information from any information-processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the Minister or appropriate law enforcement agency of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information, where the identity of that person is known to the intermediary.

(2) Where the Minister is notified in respect of any information under subsection (1), the Minister may direct the intermediary to

(a) remove the electronic record from any information-processing system within the control of the intermediary;

(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic record; and

(c) cease to provide services in respect of that electronic record.

Section VII

(3) An intermediary is not liable, whether in contract, tort, under statute or pursuant to any other right, to any person, including any person on whose behalf the intermediary provides services in respect of information in an electronic record, for any action the intermediary takes in good faith in exercise of the powers conferred by, or as directed by the Minister under, this section.

Belize – NONE

Dominica – NONE

Dominican Republic – NONE

Grenada* – LIMITED (GOOD) – Comprehensive provisions in line with best practices
[Electronic Transactions Bill, 2008]
****

34. (1) In this section, "intermediary" means a person who sends, receives or stores an electronic document, or provides other services in relation to that document on behalf of another person.

(2) An intermediary shall not be held liable in any civil or criminal proceedings for any information contained in an electronic document in respect of which the intermediary provides services, if the intermediary-

(a) is not the originator of the document;
(b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in relation to the document; and
(c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

(3) Nothing in this section shall be construed as

(a) requiring an intermediary to monitor any information contained in an electronic document in order to establish knowledge of any act, omission, fact, or circumstances giving rise to civil or criminal liability or imputing knowledge of such liability; or
(b) relieving an intermediary from complying with any law, court order, ministerial direction or contractual obligation in respect of an electronic document.

(4) Subsection (5) shall apply in any case where, in relation to information contained in an electronic document in respect of which the intermediary provides services, the intermediary has

(a) actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in respect of the document; or
(b) knowledge of an facts or circumstances from which the likelihood of such civil or criminal liability ought to have been known.

(5) The intermediary shall forthwith remove the document from any electronic communications system with the intermediary's control and shall cease to provide services in relation to that document.

(6) An intermediary shall not be liable for any act done in good faith pursuant to the provisions of this section.

Guyana – NONE

Haiti – NONE

Section VII

Jamaica – GOOD – Comprehensive provisions in line with best practices.
[Electronic Transactions Act, 2006]
****

25. (1) In this section, "intermediary" means a person who sends, receives or stores and electronic document, or provides other services in relation to that document, on behalf of another person

(2) An intermediary shall not be held liable in any civil or criminal proceedings for any information contained in an electronic document in respect of which the intermediary provides services, if the intermediary –

(a) is not the originator of the document;
(b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in respect of the document; and
(c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

(3) Nothing in this section shall be construed as –

(a) requiring an intermediary to monitor and information contained in an electronic document in order to establish knowledge of any act, omissions, facts or circumstances giving rise to civil or criminal liability; or
(b) relieving an intermediary from complying with any law, court order, ministerial direction or contractual obligation in respect of an electronic document

(4) In relation to information contained in an electronic document in respect of which the intermediary provides services , if the intermediary has –

(a) actual knowledge or the act or omission that gives rise to the civil or criminal liability, as the case may be, in respect of the document; or
(b) knowledge of any facts or circumstances form which the likelihood of such civil or criminal liability ought reasonably to have been known,

the intermediary shall be forthwith remove the document from any electronic communications system within the intermediary's control and shall cease to provide services in relation to that document.

(5) An intermediary shall not be liable for any act done in good faith pursuant to the provisions of this section.

Saint Kitts and Nevis – NONE

Saint Lucia – LIMITED (FAIR)
[Electronic Transactions Bill, 2007]
****

43. An intermediary or an internet service provider, who provides a conduit shall not be liable for the content of electronic records id the intermediary or internet service provider has no actual knowledge or is not aware of the facts that would to a reasonable person indicate as likelihood of civil or criminal liability on respect of material on the intermediary network or who, on acquiring actual knowledge or becomes aware of such facts, follows procedures required by the Regulations as soon as possible.

Section VII

Saint Vincent and the Grenadines – GOOD – Comprehensive provisions in line with best practices
[Electronic Transactions Act, 2007]
****

51. In this Part, "service provider" means any person providing information system services.

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

(2) The Minister may only recognize a representative body referred to in subsection (1) if the Minister is satisfied that:
(a) its members are subject to a code of conduct;
(b) the code of conduct requires continued adherence to adequate standards of conduct; and
(c) the representative body is capable of monitoring and enforcing its code of conduct adequately.

53. The limitations on liability established by this Part apply to a service provider only if:
(a) the service provider is a member of the representative body referred to in section 52; and
(b) the service provider has adopted and implemented the official code of conduct of that representative body.

54. (1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider:
(a) does not initiate the transmission;
(b) does not select the addressee;
(c) performs the functions in an automatic, technical manner without selection of the data;
(d) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted 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) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

55. (1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider:
(a) does not modify the data;
(c) complies with the conditions on access to the data;
(c) complies with rules regarding the updating of the data, specified in a manner widely recognized and used by the industry;
(d) does not interfere with the lawful use of technology, widely recognized and used by the industry, to obtain information on the use of data; and
(e) removes or disables access to the data it has stored upon receiving a notification referred to in section 57.

Section VII

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

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

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

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

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

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

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

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

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

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

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

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

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take down notification is to his knowledge true and correct; and

(i) an undertaking given by the complainant to indemnify the service provider from any liability incurred as a result of remedial action taken by it in complying with the notification.

58. When providing the services contemplated in this Part, there is no general obligation of a service provider to:

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

59. This Part does not affect:

(a) any obligation founded on an agreement;

(b) the obligation of a service provider under a licensing or other regulatory regime.

Suriname – NONE

Section VII

Trinidad and Tobago – LIMITED (GOOD) – Comprehensive provisions in line with best practices.
[Electronic Transactions Bill, 2009]
****

50. An intermediary or telecommunications service provider who merely provides a conduit for the transmission of electronic data messages shall not be liable for the content of electronic data messages if the intermediary or telecommunications 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 intermediary network or who, upon acquiring actual knowledge or becoming aware of such facts, follows the procedures required by section 51 as soon as practicable.

51. If an intermediary or telecommunications service provider has actual knowledge that the information in an electronic record or data message 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, the intermediary or telecommunications service provider shall as soon as practicable–
(a) notify the Telecommunications Authority of Trinidad and Tobago and if it considers it appropriate, notify the appropriate law enforcement authorities of the relevant information;
(b) where authorized by written law, disclose the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary; and
(c) where authorized by written law, remove the information or data message from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information or take any other action authorized by law.

International Best Practices and Regional Trends

European Union

Directive 2000/37/EC

Section 4: Liability of Intermediary Service Providers

Article 12 – "Mere Conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Section VII

Article 13 – "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
   (a) the provider does not modify the information;
   (b) the provider complies with conditions on access to the information;
   (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
   (d) the provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and
   (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 – Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
   (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 – No General Obligation to Monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2 Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Section VIII:
Summary of Assessment of Regional Texts

Provided on the overleaf is a summary of the major findings coming out of the comparisons undertaken in Section 7 above.

In view of the ultimate objective of the HIPCAR project is the harmonization of regional policy and legislative frameworks, pursuant to the review outlined below the following areas of significant divergence were identified:

(i) Definition of key elements

There needs to be consensus on the meaning and use of the following terms:

(a) whether "***electronic records***" should be defined with as wide an application as in, for example, Jamaica as compared to the definitions such as in Trinidad and Tobago's draft which explicitly identified "***electronic data message***" separate and apart from "electronic record" which has more specific scope. This difference seems to be based on particular obligations relating to a particular type of document – a record of an electronic transaction – as opposed to the substantive document itself.

(b) "*certificate service providers*," and/or related terms such as "*encryption service providers*" and "*information security service providers*", and whether these contemplate the same things. There needs to be harmonization of the expected description, titles and roles of these parties as strictly speaking such persons an be assumed provide related but distinct information society products within the security sphere.

(ii) Categories of documents excluded from applicability of the Act

While there is agreement on the exclusion of applicability to wills, trusts , transfers in real property, and power-of attorney among frameworks, some of the other the exclusions suggested in some frameworks and not in others include:

(i) negotiable instruments;
(ii) court orders; and
(iii) national documents related to immigration, citizenship or passport matters.

A coherent identification of exempted documents across the region should be developed as a means of harmonizing the scope of legislative instruments.

(iii) Electronic signatures and administration of Certificate Service Providers

Despite general consensus on the means tests of what would constitute a qualified certificate, and the recognition that qualified certificates issued from anywhere should be recognized, there are variances in the approaches of market access and oversight among Beneficiary States – tending from fairly open models of entry requiring registration with the oversight body, through approaches that are strictly regulated and requiring application and approval processes, and in at least one case, the apparent establishment of a state-sponsored monopoly. The regulatory philosophy must be harmonized across the region, outlining the general administrative objective, much like that expressed by the EU in its Directive which explicitly instructed member states to limit market entry barriers, be they tariff-based or otherwise.

Similarly, there is a variety of approaches to the recognition of signatures, best practice suggests the recognition of a variety of signatures with increasing sophistication resulting in being validation for more sterner legal conditions. The approach is inconsistently applied throughout the region, with some jurisdiction's legislation tacitly limiting the type of signatures to be identified. Again, the need to regularize a single region-wide philosophy and regulatory objective is essential going forward.

(iv) Customer protection

Unlike many of the jurisdictions. Jamaica and St. Vincent and the Grenadines are unique for the inclusion among the customer protection provisions of a "cooling off" period within which consumers may withdraw the online contract without penalty. This provision seems based on Article 6 of the EU Directive 97/7/EC on consumer protection for 'distance contact' purchases. Despite telephone based transactions were referred to in the recitals of that Article, there should be the consideration that blanket application of such a provision over most electronic transactions may act as a disincentive for vendors. In the context of the appropriate balance in the framing of such a provision, as this is generally a matter of larger consumer protection policy, there must be consideration of whether such is appropriate for inclusion in e-commerce frameworks.

Summary Chart of Key Elements and Status

Country/Region	1. Legal Mandate	2. Legal Effect of Electronic Transactions	3. Legal Requirements for the Validity of e-Documents	4. Contracts Formation	5. Electronic Signatures	6. Consumer Protection	7. Intermediaries and Telecommuni-cations Providers
Antigua and Barbuda	LIMITED (GOOD)	LIMITED (GOOD/FAIR)	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (FAIR)	LIMITED (FAIR)	LIMITED (GOOD)
Bahamas	GOOD	GOOD	GOOD	GOOD	POOR	NONE	GOOD
Barbados	GOOD	GOOD (FAIR)	GOOD	FAIR	GOOD (FAIR)	NONE	GOOD
Belize	FAIR	GOOD	GOOD	GOOD	NONE	GOOD	NONE
Dominica	NONE	NONE	NONE	NONE	NONE	FAIR	NONE
Dominican Republic	GOOD	NONE	GOOD	GOOD	GOOD	NONE	NONE
Grenada	LIMITED (FAIR)	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (FAIR)	LIMITED (GOOD)	LIMITED (GOOD)
Guyana	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	GOOD (FAIR)	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
St. Kitts and Nevis	NONE	NONE	NONE	NONE	NONE	NONE	NONE
St. Lucia*	LIMITED (FAIR)	LIMITED (GOOD)	LIMITED	LIMITED (GOOD)	LIMITED (FAIR)	LIMITED (GOOD)	LIMITED (FAIR)
St. Vincent and the Grenadines	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
Suriname	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago*	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (GOOD)	LIMITED (FAIR)	LIMITED (GOOD)	LIMITED (GOOD)

* Bills laid before Parliament, not yet passed as statute (as of March 2010).

ANNEXES

Annex 1: Glossary

Beneficiary Countries	Beneficiary Countries of the ITU/EU-funded HIPCAR Project
B2B	Business to Business
B2C	Business to Consumer
C2C	Consumer to Consumer
ITU	International Telecommunication Union
EC	European Commission
E-Commerce	Electronic Commerce
EU	European Union
ETA	Electronic Transactions Act, Barbados
G2C	Government to Consumer
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedures
ISP	Internet Service Provider
OECS	Organisation of Eastern Caribbean States
OECD	Organisation for Economic Co-operation and Development
UECA	Uniform Electronic Commerce Act, United States of America
ULCC	Uniform Law Conference of Canada
UNCITRAL	United Nations Commission on International Trade
UN	United Nations

Annex 2: Bibliography

1 Electronic Transactions Actl 2006, Jamaica www.laws.gov.ag/bills/2006/electronic-transactions-bill-2006.pdf

2 Electronic Transactions and Communications Bill- www.ictparliament.org/index.php/component/legislationlibrary/?task=

3 Electronic Transactions Act, Cap. 308B www.caricomlaw.org/docs/Electronic%20Transactions.pdf

4 See notes on Barbados Electronic Transactions Act found at http://cc.bingj.com/cache.aspx?q=ectronic+transactions+act+un&d=76785265090955&mkt=en-US&setlang=en-US&w=824f0bb6,1b10a9d7

5 The Electronic Transactions Act, Jamaica, (Power Point Presentation) Myers, Fletcher & Gordon, Attorneys-at-law

6 Harmonization of the Legal Framework Governing ICTs in West African States, Economic Community of West African States, United Nations Economic Commission for Africa, West African Economic and Monetary Union, by Abdoullah CISSE, University Professor Consultant July 2007

7 United Nations Conference on Trade and Development Information Economy Report 2007-2008, Science and technology for development: the new paradigm of ICT Prepared by the UNCTAD Secretariat UNITED NATIONS New York and Geneva, 2007.

8 13th Meeting of the Intergovernmental Committee of Experts (ICE), Mahe, Seychelles, 27-29 April 2009 Ad Hoc Expert Group Meeting : "Harmonization of ICTs Policies and Programmes in Eastern Africa Subregion and Prospects" , United Nations Economic Commission for Africa Subregional Office for Eastern Africa.CA.

9 Cybercrime Legislation Resources, ITU Toolkit for Cybercrime legislation , developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector, Draft April 2009.

10 Annex 4 Contribution by Professor Michael Geist University of Ottawa, Faculty of Law, Director of E-commerce Law, Goodmans LLP, found on www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc

11 Murray, Andrew (2004) "Regulating Electronic Contracts: Comparing the European and North American Approaches"

Additional Websites

12 www.central-bank.org.tt/publications/issues/sft1242052240.pdf

13 www.ictregulationtoolkit.org/en/Section.2107.html

14 www.itu.int/osg/spu/ni/ubiquitous/Presentations/10_lam_dataprotection.pdf

15 http://peterfleischer.blogspot.com/2009/01/launching-another-global-forum-to-talk.html

16 www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution international_standards_en.pdf

17 www.itu-coe.ofta.gov.hk/vtm/ict/faq/q10.htm

18 www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

19 www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf

20 www.itu.int/ITU-T/newslog/New+Report+On+Lawful+Interception.aspxhttp: //www.itu.int/ITU-

Annex 3:

Participants of the First Consultation Workshop for HIPCAR 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
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir

Annex 3

Country	Organization	Last Name	First Name
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / International Organizations' Participants

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

HIPCAR Project Experts

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[8]	J Paul
PRESCOD	Kwesi

[8] Workshop Chairperson

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013