UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Towards e-commerce legal harmonization in the Caribbean

UNITED NATIONS

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Towards e-commerce legal harmonization in the Caribbean

UNITED NATIONS
New York and Geneva, 2017

© 2017, United Nations

This work is available open access by complying with the Creative Commons licence created for intergovernmental organizations, available at http://creativecommons.org/licenses/by/3.0/igo/.

The interpretations and conclusions expressed herein are those of the authors and do not necessarily r States.

The designation employed and the presentation of material on any map in this work do not imply the expression of any opinion whatsoever on the part of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Photocopies and reproductions of excerpts are allowed with proper credits.

This publication has been edited externally.

United Nations publication issued by the United Nations Conference on Trade and Development.

UNCTAD/DTL/STICT/2017/9

NOTE

Within the UNCTAD Division on Technology and Logistics, the ICT Analysis Section carries out policy-oriented analytical work on the development implications of information and communication technologies (ICTs) and electronic commerce. It is responsible for the preparation of the *Information Economy Report* (IER) as well as thematic studies on ICT for Development, including regional comparative reviews on e-commerce legislation. The ICT Analysis Section promotes international dialogue on issues related to ICTs for development, and contributes to building developing countries' capacities to measure the information economy and to design and implement relevant policies and legal frameworks. Since 2015, it has mapped e-commerce legislation in the areas of e-transactions, data protection, cybercrime and consumer protection online (unctad.org/cyberlawtracker). The ICT Analysis Section is also responsible for the coordination of *eTrade for all* (etradeforall.org), a new multi-stakeholders' initiative launched at UNCTAD 14 in July 2016, which aims to improve the ability of developing countries, and particularly least developed countries, to use a om e-commerce.

This publication has been edited externally.

The following symbols have been used in the tables:

Two dots (..) indicate that data are not available or are not separately reported. Rows in tables have been omitted in those cases where no data are available for any of the elements in the row;

A dash (-) indicates that the item is equal to zero or its value is negligible;

Reference to "dollars" (USD) means United States of America dollars, unless otherwise indicated;

Details and percentages in tables do not necessarily add up to the totals because of rounding.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers of boundaries.

The material contained in this study may be freely quoted with appropriate acknowledgement.

PREFACE

UNCTAD is mandated to help developing countries in the of ICTs and e-commerce and, since 2002, has been the leading capacity-building provider within the United Nations system supporting the preparation of legal frameworks for e-commerce through the E-Commerce and Law Reform Programme and TrainForTrade Programme of the Division on Technology and Logistics.

Security and trust are fundamental for creating an environment conducive to e-commerce. Online fraud and data breaches are growing concerns for both consumers and enterprises, requiring adequate legal responses at national and international levels. The lack of legal frameworks in several regions, including in Caribbean countries, is impeding the development of e-commerce.

In the Latin American and Caribbean region, UNCTAD has carried out since 2007 joint capacity-building activities in the of e-commerce with the support of Spain and Finland, in cooperation with the Secretariat of the Latin American Integration Association (ALADI); the Latin American and Caribbean Economic System (SELA) and with the Association of Caribbean States (ACS). Some of these activities included on-line distance learning courses and regional training sessions that over 1,200 lawmakers, government and practitioners involved in the business aspect of e-commerce from the public and private sectors. Moreover, UNCTAD has published two studies in the region entitled "*Study on Prospects for Harmonizing Cyber-legislation in Latin America (2015, 2009)*" and "*Study on Prospects for Harmonizing Cyber-legislation in Central America and the Caribbean"(2009)*.

The purpose of this publication is to provide up-to-date information on the legal framework of Caribbean countries following the Regional Workshop on E-Commerce Legislation Harmonization in the Caribbean held from 29 September to 2 October 2015 in Port of Spain, Trinidad and Tobago. The workshop was sponsored by the Government of the Republic of Trinidad and Tobago, SELA, ACS and the Government of Finland.

participants from the following Caribbean countries took an active part in workshop: Antigua and Barbuda, Bahamas, Barbados, Costa Rica, Cuba, El Salvador, Jamaica, Saint Lucia, Suriname, and Trinidad and Tobago. Prior to the workshop, a TrainForTrade distance learning course on legal aspects of e-commerce had been delivered in March/April 2015 with the participation of 140 representatives from 21 countries in the region.

This study reports on progress made by the countries in regard to electronic transactions/electronic signatures, online protection of consumers, protection of personal data, industrial and intellectual property, domain names, cybercrime, security of information and pending legislation and challenges.

I would like to express my sincere appreciation to all who have contributed to the process and thank development partners for their continuous support to UNCTAD Programme on E-Commerce and Law Reform.

It is my hope that this study will further reinforce the capabilities of Member States to develop electronic commerce legislation to allow for more online trade at the domestic, regional but also international levels.

Shamika N. Sirimanne

Director, Division on Technology and Logistics, UNCTAD

ACKNOWLEDGMENTS

This study was prepared as part of the work of the Science and Technology and Information and Communication Technology Branch in close co-operation with the TrainForTrade Programme of the Division of Technology and Logistics of UNCTAD.

The study's principal consultant was Ian Walden. The study was prepared by a team from UNCTAD comprising Gonzalo Ayala, Cécile Barayre and Torbjörn Fredriksson. Statistical support was provided by Smita Lakhe. We are grateful for the contributions made by participants in the regional workshop on e-commerce legislation harmonization in the Caribbean, held in Port of Spain, Trinidad and Tobago in 2015: Mazuree Colin Ali, Pablo Ernesto Ayala Monges, Allison Bidaisee, Shelley-Ann Clarke-Hinds, Coppin, Georgette Crane, Craig Douglas, Alexis Downes-Amsterdam, Jan Drysdale, Alberto Durán Espaillat, Luxmore Edwards, Makisleidis Esponda Bravo, John D. Gregory, Shermatie Jagdeo, Hellen Jimenez, Justin John, Charelle Joseph-Samaroo, Caitlin Karijokromo, Chamyantie Lal, Nayelly Loya, Christian Marquez, Wilfred McKenzi, Philip McClauren, Tricia Puckerin, Sunita Ramsumair, Sheila Seecharan, Shirley Sheppard, Rene Singh, David Satola, Bridgid Sutherland, Anthony V. Teeluck-singh, Bobby Williams, and Deon Woods Bell.

National inputs provided by representatives of UNCTAD member states are greatly appreciated, as well as inputs received from the Economic Commission for Latin America and the Caribbean (ECLAC).

The cover was prepared by Nadège Hadjemian. Desktop publishing and graphics were executed by Nathalie Loriot of the UNOG Printing Section. The report was edited by Nancy Biersteker.

Financial support by the Government of Finland is greatly appreciated.

ABBREVIATIONS

ACS	Association of Caribbean States
AMCHAM	American Chamber of Commerce
AMI	Mesoamerican Information Highway
B2C	Business to Consumer
CAF	Development Bank of Latin America
CARICOM	Caribbean Community
ccTLD	Country Code Top-level Domain
CMA	Computer Misuse Act
CoE	Council of Europe
CTU	Caribbean Telecommunication Union
DPA	Data Protection Act
ECA	Electronic Crimes Act
ECLAC	Economic Commission for Latin America and the Caribbean
ECT	Electronic Communications and Transactions Act
ECTEL	Eastern Caribbean Telecommunications Authority
EGRIP	Electronic Government for Regional Integration Project
ETA	Electronic Transactions Act
ETECSA	Empresa de Telecommunicaciones de Cuba S.A.
EU	European Union
FOIA	Freedom of Information Act
GDP	Gross Domestic Product
HIPCAR	Harmonization of ICT Policies and Legislation Across the Caribbean
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	Information and Communication Technologies
IER	Information Economy Report
IoT	Internet of Things
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
LACNIC	Latin America and Caribbean Network Information Centre
MIC	Ministry of Informatics and Communications (Cuba)
MICIT	Ministry of Science and Technology (Costa Rica)
MINCOM	Ministry of Communications (Cuba)
MITS	Mona Information Technology Services (Jamaica)
NTRC	National Telecommunications Regulatory Commission (Saint Lucia)
OECS	Organisation of Eastern Caribbean States
PRODHAB	Agencia de Protección de Datos de los Habitants (Costa Rica)
SELA	Sistema Económico Latinoamericano y del Caribe
TA	Telecommunications Act
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNCITRAL	United Nations Commission on International Trade Law
USD	United States Dollar

CONTENTS

PART I
REFORMING CYBERLAWS IN THE CARIBBEAN

A. INTRODUCTION

The establishment of adequate legal frameworks can facilitate the transition to a digital economy and the take-up of e-commerce in-country but also regionally and internationally by reducing uncertainties, enhancing trust and addressing potential harms. With rising use of e-commerce and current developments in cloud computing, the Internet of Things ('IoT') and big data, the need for such frameworks has become urgent. According to the UNCTAD Global Cyberlaw Tracker, 77 per cent of countries have adopted a law on electronic transaction, 72 per cent on cybercrime, 52 per cent on privacy and data protection and 50 per cent on the protection of consumers online.

Across the Caribbean region, there have been a number of initiatives aiming at fostering the use of information and communications technologies (ICTs) and this report examines the legal and regulatory framework for e-commerce in 10 countries: Antigua and Barbuda, Bahamas, Barbados, Costa Rica, Cuba, El Salvador, Jamaica, Santa Lucia, Suriname and Trinidad and Tobago. It examines the current state of a number of key areas of law and regulation for e-commerce and cyber-related activities.

1. Electronic transaction laws

Electronic transaction laws can cover a wide range of issues, all of which are primarily designed to facilitate e-commerce. First, legal recognition is granted to electronic means of communication, where such communications have legal effect, either in the process of contract formation, to evidence acts or to meet administrative requirements. The latter is often tied to a policy of promoting e-government initiatives, which is seen as helping to reduce the cost of interfacing with the public sector for both citizens and business.

Electronic signature and regimes are often established under an electronic transaction law. Electronic or digital signatures are seen as ensuring authentication and integrity of electronic communications, which are often seen as less reliable or secure than traditional paper-based procedures. can involve the use of third party service providers to act as trusted intermediaries between the various communication parties.

2. Consumer protection

Consumer protection regimes operate under the assumption that the consumer is the weaker party and needs protection from unscrupulous practices by suppliers. Such possibilities are seen as being greater in a cyberspace environment, where the parties operate at a distance and with unknown online entities. Statutory protections can give consumers greater to go online, through measures such as increased transparency and payment protection rules. Enhancing consumer in e-commerce should lead to the development of transparent and effective consumer protection mechanisms, ensuring a level of protection that is not less than that afforded in other forms of commerce. It often implies the review of existing consumer protection laws and frameworks to accommodate the special features of e-commerce, such as the ease, speed and discretion with which businesses and consumers can communicate, and ensure that consumers and businesses are informed and aware of their rights and obligations in the digital marketplace.

3. Data protection

As personal data have become the fuel of the cyber-economy, users have become increasingly concerned about the use and abuse of their personal data. In response, data protection laws try to redress the balance, similar to consumer protection laws, by giving users greater control over their personal data. Such laws are also becoming a critical issue for the transbor

4. Cybercrime

The prevention of cybercrime often requires the existing criminal law and criminal procedure to be updated to r the new forms of criminal conduct, such as hacking and viruses, and to grant law

enforcement new powers to investigate, prosecute and disrupt such criminality. Building the capacity, reducing vulnerabilities and hardening targets at both an infrastructure and individual level remain some of the most effective ways to help countries address the challenges of cybercrime and electronic evidence. In addition, the development of domestic legal frameworks for combating cybercrime should not be done in isolation. Compatibility of such laws and policies at the regional and international level is desirable. The establishment of common minimum standards can help ensure cross-border coordination on the design and implementation of relevant legislation and enforcement mechanisms. The judiciary and the police would from cooperating at the international level.

5. Online content

Traditional content regulation has focused on the media, broadcast and newspapers. In cyberspace, content can be generated and made available by anyone and everyone using a wide range of different platforms and intermediary service providers. To facilitate content creation and dissemination, while protecting intermediaries from liability for third-party content, rules have been adopted requiring intermediaries to exercise control in circumstances while not being obliged to monitor all content made available via their services. However, a key question that arises in relation to the role of Internet Service Providers is whether they should be held liable in respect of content that they provide access to, caches or hosts? Second, if such liability does exist, what are its limits? If ISPs were to be held liable for all content to which they provide access, then they are less likely to offer such services, which would be to the detriment of the development of e-commerce. An appropriate balance therefore needs to be achieved.

6. Domain names

The regulatory issue covered in this report is the management of the Top-Level Country Domain Names within each country, as a critical resource for domestic players and international investors. IPv6 (Internet Protocol version 6) is the most recent communications protocol providing and user location. IPv6 readiness varies greatly in the region and less than 1 per cent of all users in the Caribbean are ready to operate in IPv6.[1]

B. HARMONIZATION INITIATIVES

As a truly global environment, cyberspace is challenging national legal and regulatory regimes. To try to maintain standards of protection, reduce the patchwork of different applicable rules and to prevent the growth of 'cyber-havens', numerous inter-governmental organizations and lawmakers have engaged in various harmonization initiatives; creating model laws, conventions and other instruments to which states can either formally ascribe, through signature and procedures, or informally use as a precedent for regional or domestic reform activities.

In each of the areas outlined above, there is one or more key instruments that have tended to dominate the reform agenda in the region.

- For electronic transactions, the United Nations Commission on International Trade Law (UNCITRAL) has been most active, adopting Model Laws on electronic commerce (1996) and electronic signatures (2001), as well as promoting the UN Convention on the Use of Electronic Communications in International Contracts (2005). Nine of the 10 countries in this report have based their legislation on a UNCITRAL Model. Antigua and Barbuda, Barbados, Jamaica and Saint Lucia have implemented both the Model Law on Electronic Commerce and the Model Law on Electronic Signatures, while Trinidad and Tobago's e-transaction law is based on both of the two Model Laws as well as the 2005 Convention. Suriname has drafted a law that is based on both UNCITRAL Model Laws, while the Bahamas only use the Model Law on Electronic Commerce and El Salvador has based its e-transaction law only on the Model Law on Electronic Signatures.

For data protection, the European Union Data Protection Directive (1995) has dominated international debates, largely due to its controls over the transfer of personal data to non-EU countries. Other key instruments include the Commonwealth Model Laws on Privacy, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention 108), which is also open to non-European countries.

- The Council of Europe Convention on Cybercrime (2001) remains the leading international standard in the area of cybercrime and cyber protection. Antigua

and Barbuda's legal framework seems generally harmonized with the Council of Europe Convention on Cybercrime and Saint Lucia's Computer Misuse Act r ovisions of the Convention.

- Relevant international guidelines and standards on e-commerce were produced by the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce revised in 2016. The United Nations Guidelines on Consumer Protection refer to the OECD guidelines.
- In the cases of online content and domain names, there is no international reference text. The regulation of Internet content is a complex area, not least due to the cross-border nature of the Internet, with overlapping jurisdictions each seeking to enforce differing levels of control over information and cultural differences that inform much national information control legislation.

At a regional level, various initiatives aiming at fostering the use of ICTs have been pursued and faced several challenges. Box 1 refers to two main initiatives led by the International Telecommunication Union (ITU) with the HIPCAR Project to support harmonizing approaches to ICT development and the Economic Commission for Latin America and the Caribbean (ECLAC), which produced a study that examines past efforts in the region at collaboration in the context of e-government projects.

Box 1. Regional initiatives: The ITU HIPCAR Project and the ECLAC study on the "Regional approaches to e-government initiatives in the Caribbean"

The Harmonization of ICT Policies and Legislation Across the Caribbean (HIPCAR) Project aims to support Caribbean countries in improving their competitiveness by harmonizing approaches to ICT development. It was launched in 2008 after having been conceived by the ITU, the Caribbean Community (CARICOM) Secretariat, and the Caribbean Telecommunication Union (CTU). Stakeholders include government representatives, regulators, civil society, academia and the private sector.

HIPCAR has developed draft regional model policy guidelines for two priority areas: 1) ICT legislative framework, which includes e-transactions and evidence, access to public information, privacy and data protection, cybercrimes and cybersecurity, as well as the interception of communications; and 2) telecommunication acts, including universal service and access framework, the licensing in a convergent environment, and interconnection including cost modeling.

In the following, in-country technical assistance was made available to transform the regional guidelines into national legislative and regulatory frameworks. Target countries have been Barbados, Grenada, Haiti, Jamaica, Saint Christopher and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago.

As part of a 2016-released study entitled Regional approaches to e-government initiatives in the Caribbean, ECLAC examined past efforts at collaboration among Caribbean countries in the context of e-government projects. It reviewed a number of regional initiatives in this area, which included efforts to produce model legislation, such as through the ITU Harmonization of ICT Policies and Legislation Across the Caribbean (HIPCAR) project and parts of the Electronic Government for Regional Integration Project (EGRIP). The study revealed that these regional initiatives have met with equently fall short of their initial goals.

A lack of follow-through was as a problem – often exacerbated by the project based nature of these initiatives. An example is the case of HIPCAR, where much work was completed to craft a common set of model laws, but these laws have yet to receive an CARICOM endorsement. Having run its course, there is no concerted push to integrate these models into Caribbean legislation.

The ECLAC study did note some bright spots. For example, the EGRIP programme helped to establish e-tax systems – and the legislation to support them – in several countries of the Organisation of Eastern Caribbean States (OECS). Another encouraging example is the work of the Eastern Caribbean Telecommunications Authority (ECTEL), which is an institution that enables the harmonization of regulatory policy for telecommunications across States of the OECS – Dominica, Grenada, Saint Kitts and Nevis, Saint Lucia, and Saint Vincent and the Grenadines. As an advisory body to national regulators, ECTEL has provided crucial support to enable its members to expand network connectivity and maintain competition in telecommunications markets.

In general, the study found that "those projects most likely to succeed are carefully targeted to address common problems, have commitment from partner countries, and build upon pre-existing legal and institutional frameworks for collaboration."

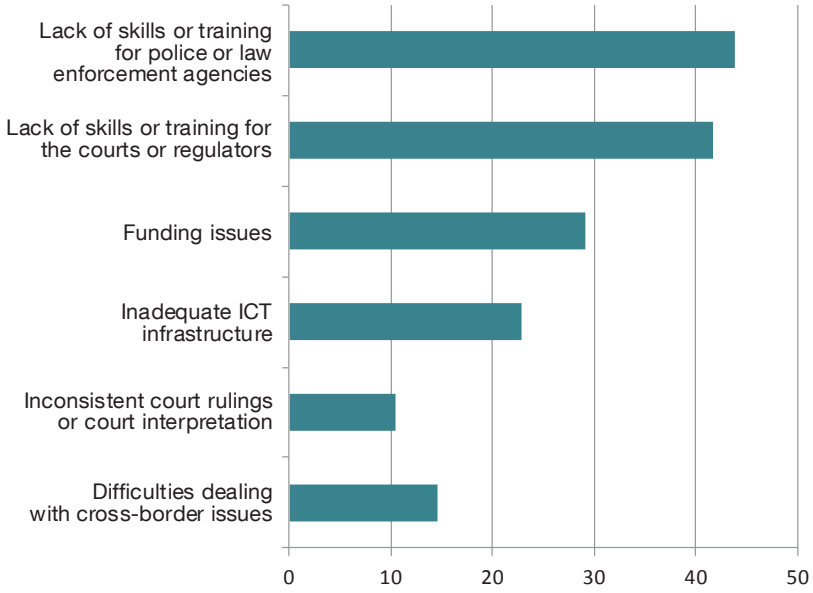
Source: ITU, 2008, http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx and ECLAC, 2016, repository.eclac.org/bitstream/handle/11362/39858/S1501269_en.pdf?sequence=1&isAllowed=y.

From experience in other jurisdictions, addressing the process of effective law reform will often involve a number of elements and steps. First, there is the need for express political commitment to the law reform process at the highest level of governments. Second, a relevant government ministry must claim ownership of the matter and be prepared to devote internal resources, both to carry out the necessary work internally as well as liaise and co-ordinate actively with other relevant stakeholders in the process, including other ministries, relevant agencies, the private sector and civil society. A third element is the need to identify and appoint relevant technical and legal expertise to support the lead ministry, internal to the authority and/or external, whether located nationally or internationally. The work of the expert(s) must then be supported through the establishment of a stakeholder review group, chaired by the lead ministry, including representation from the public and private sectors. Obvious potential candidates include people from the ministry of justice, the national law reform commission and local commercial and legal practitioners. Any draft measures prepared by the experts would then be subjected to a process of scrutiny by the stakeholder review group, which should both substantially improve the quality of the draft and facilitate awareness and build support for the proposal among the wider community. The draft measure should be steered through the parliamentary process by the lead ministry, ensuring that steps are taken to fully explain the purpose, nature and consequences of the measure to the political representatives. Finally, the next challenge lies in enforcement of the laws. Based on UNCTAD's experience in different developing regions (Figure 1), there is a need to strengthen the capacity of enforcement in order to enforce the legislation.

As part of the discussions among participating countries at the "Regional Workshop on E-Commerce Legislation Harmonization in the Caribbean" organized by UNCTAD in 2015, there was an agreement that the reform process requires commitment from the highest levels of each State to facilitate the effective revision and adoption of legal texts. UNCTAD recommended that the following steps be taken by Caribbean States to facilitate the legislation process:

- undertaking a cyberlaw audit in order to assess the need for legal revision;
- establishing a benchmark analysis based on international, regional and national best practice;
- drafting preliminary legislation to guarantee coherence with existing legal documents, internally, regionally and internationally;
- adopting the legislation; and

Figure 1. Challenges to the enforcement of e-commerce legislation in the ASEAN and selected Latin America and Caribbean countries, 2013-2015 (percentage of respondents)



Source: UNCTAD, 2016

- developing guidelines for domestic enforcement of the legislation.

UNCTAD recommends that member States share contacts and best practices among themselves, especially resources for shared and development of domestic and cross-border e-commerce. This could be achieved through informal and formal mechanisms at national and regional levels to advance the e-commerce legislation harmonization, as well as by engaging participants to become the promoters of law reform.

C. ICT AND E-COMMERCE UPTAKE IN THE REGION

Disparities in ICT uptake in the Caribbean remain substantial, with great variations in the use of the Internet. The use of the Internet and the percentage of broadband subscriptions have constantly increased in all countries over the last years. Barbados and the Bahamas rank – with almost 80 per cent of the population using the Internet and more than 20 per cent having a broadband subscription. Recently, active mobile broadband subscriptions have notably increased, especially in Costa Rica, where it has reached approximately 97 per cent in 2015. Active mobile broadband subscriptions have been stagnant in Cuba, where no one uses this technology, and the increase has been smaller in El Salvador and the Bahamas, reaching about 20per cent in 2015. Mobile penetration is very high but has been stagnant or decreasing in most countries over the last years. It is highest in Suriname and Trinidad and Tobago, where the percentage of mobile cellular subscriptions has been increasing steadily up to approximately 181 per cent in Suriname and 158 per cent in Trinidad and Tobago. The percentage of telephone subscriptions has been stagnant or falling in most countries as well.

Table 1. Key ICT statistics in the Caribbean in 2015

	Individual using the Internet per 100 inhabitants	broadband subscriptions per 100 inhabitants	Active mobile broadband subscriptions per 100	Number of mobile cellular subscriptions per 100 inhabitants	telephone subscriptions per 100 inhabitants
Antigua and Barbuda	65.20	13.07	33.8	137.22	13.07
Bahamas	78.00	20.91	21.1	80.29	31.20
Barbados	76.11	27.23	54.9	116.46	54.56
Costa Rica	59.76	11.17	97.2	150.66	17.18
Cuba	31.11	0.07	-	29.65	11.52
El Salvador	26.92	5.49	19.9	145.26	14.69
Jamaica	43.18	5.83	53.5	111.51	8.98
Saint Lucia	52.35	15.37	33.6	101.52	18.86
Suriname	42.76	9.48	66.6	180.69	15.50
Trinidad and Tobago	69.20	20.68	32.9	157.67	20.11

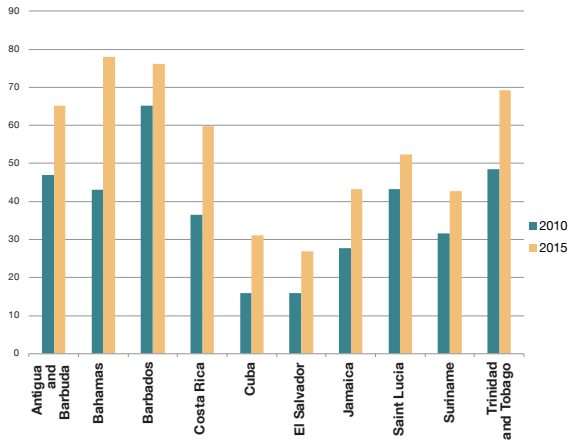
Source: ITU, 2016.

Table 2. Core Household Indicators

	Proportion of households with				Percentage of individuals using					
	computer	year	Internet access at home	year	computer	year	Internet	year	mobile	year
Costa Rica	53.2	2015	60.2	2015	47.0	2015	59.8	2015	73.0	2012
Cuba	13.0	2015	5.6	2015	29.2	2013	29.1	2014	11.3	2013
El Salvador	22.3	2013	13.9	2014	26.7	2014	24.8	2014	79.1	2014
Jamaica	32.3	2014	26.4	2014	40.3	2014	40.4	2014	90.4	2014
St. Lucia	38.4	2014	36.6	2014	..	..	45.9	2012	..	..
Suriname	42.8	2014	36.1	2014	..	..			..	..

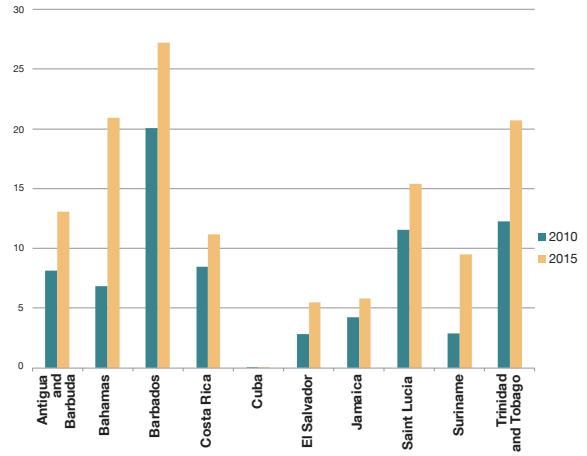
Source: ITU, 2016.

Chart 1. Individual Using Internet (%)



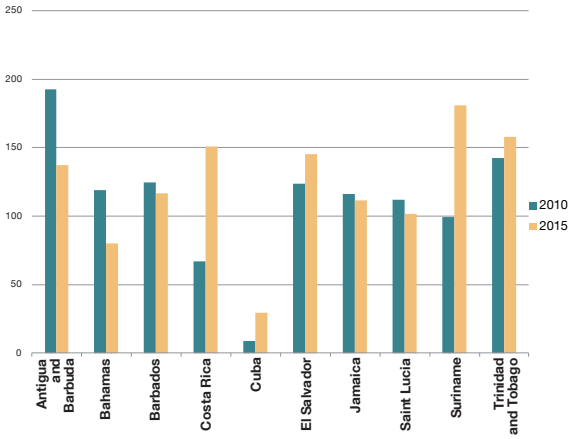
Source: ITU, 2016.

Chart 2. Fixed Broadband Subscriptions per 100



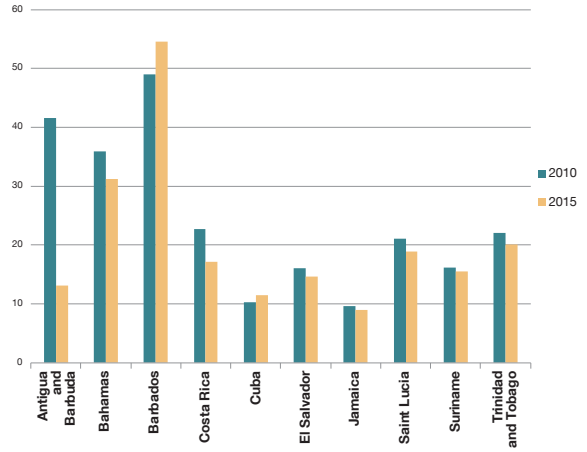
Source: ITU, 2016.

Chart 3. Mobile cellular subscriptions per 100



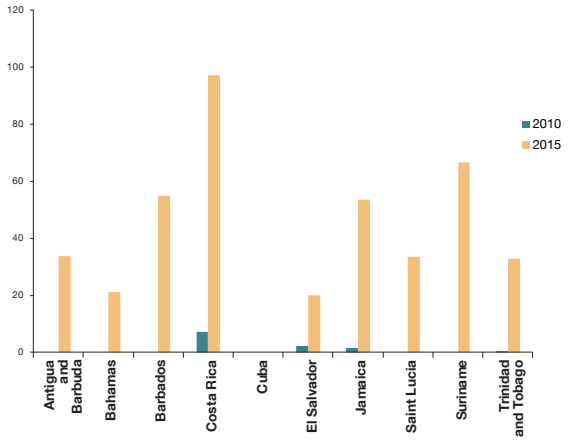
Source: ITU, 2016.

Chart 4. Fixed Telephone Subscriptions per 100



Source: ITU, 2016.

Chart 5. Active mobile broadband subscription (%)



Source: ITU, 2016.

Table 3. UNCTAD B2C e-commerce index 2016

	2016 Rank	Share of individuals using the Internet (2014 or latest)	Share of individuals with credit card (15+, 2014 or latest)	Secure Internet servers per 1 million people (normalized, 2014)	UPU postal reliability score (2013-14)	UNCTAD B2C e-commerce Index value 2015	2014 Rank
Costa Rica	55	49	14	70	76	52.4	52
Jamaica	66	41	14	66	70	47.6	80
Trinidad & Tobago	67	65	15	71	39	47.5	43
El Salvador	96	30	8	58	31	31.7	72

Source: UNCTAD, 2016.

With regard to e-commerce, four Caribbean countries – Costa Rica, Jamaica, Trinidad and Tobago, and El Salvador – were included in the geographic coverage of 137 countries of the UNCTAD B2C E-commerce Index 2016, which measures the readiness of countries to engage in online commerce (Table 3).[2] It is composed of four indicators: Internet use penetration, credit card penetration, secure servers per one million inhabitants, and a postal reliability score.

UNCTAD's B2C E-Commerce Index also measures Internet shoppers in the region. The 2016 Index compiles data for Costa Rica from 2012 and from El Salvador from 2014. The percentage of Internet shoppers of the population remains low in both countries, reaching 5 per cent in Costa Rica and 3 per cent in El Salvador. In Costa Rica, 8 per cent of the people who use the Internet have bought products or services online within the last three months, in El Salvador 8 per cent of the Internet users have bought a product online within the previous year. Private e-commerce businesses, as shown on the example of TriniTrolley in Box 3, have recently advanced in the Caribbean.

Box 3. TriniTrolley

TriniTrolley is the Caribbean's largest e-commerce business. The company was launched in 2009 to provide residents of Trinidad and Tobago with products that can be purchased through an online shopping website with under 48-hour delivery instead of long shipping times through the traditional "sky box" companies for online shopping. By 2011, the company expanded to include delivery to the rest of the Caribbean region.

Prior to TriniTrolley's launch, there were no third party credit card processors operating in the Caribbean other than PayPal in Jamaica. When PayPal offered services in Trinidad in 2011, Trini Trolley became one of its subscribers. In the same year, the company offered seller account features whereby private individuals, sole traders and businesses can sell online via the website at no cost. To date more than 39,000 seller accounts have been created with many unregistered businesses becoming registered and expanding to create their private e-commerce businesses. The number of registered customers increased from about 41,000 in 2011 to 348,000 in 2016.

TriniTrolley's opportunities to expand include establishing physical warehouse spacing in more countries in addition to furthering the partnerships with the regional banks and its long-standing relationship with MasterCard. Challenges include the laws and legislation for support of e-commerce in other Caribbean countries and the need for educating the various societies on the merits of e-commerce.

Source: TriniTrolley, January 2017.

D. CURRENT STATUS OF E-COMMERCE LAW HARMONIZATION IN THE CARIBBEAN

1. Electronic Transaction Law

Progress towards harmonization has been strongest in the area of electronic transactions laws. Seven out of 10 countries have relevant legislation in place. Cuba, El Salvador and Suriname have not yet passed electronic transaction legislation, but draft laws have been developed in all three countries.

2. Consumer Protection

Consumer protection legislation is characterized by diversion in the region. Seven out of 10 countries have enacted legislation and Saint Lucia has a partial consumer protection legislation in place, contained in its Electronic Transaction Law. Suriname and Cuba do not have consumer protection legislation to date,

however, Suriname has made progress towards a draft law.

3. Data Protection and Privacy

Only four countries - Antigua and Barbuda, the Bahamas, Costa Rica, and Saint Lucia - have enacted data protection and privacy laws. While Barbados has drafted a comprehensive Data Protection Bill, current data protection and privacy legislation is only partial in the country. Apart from Barbados, countries have partial legislation in place, but they do not provide the same level of detail and coverage as full data protection and privacy legislation.

4. Cybercrime and Cybersecurity

Cybercrime and cybersecurity is fairly harmonized in the region, with seven out of 10 countries having full legislation. In 2015, El Salvador has published a draft law on computer and cybercrime. Together with two other countries in the region – Costa Rica and Suriname – El Salvador has partial laws in place.

5. Online Content

The region lacks behind with regard to online content legislation and may need to catch up quickly. None of the 10 countries has a legislation or a draft law in place. Yet, six countries have partial online content legislation, which is entailed in their Electronic Transaction Legislation.

6. Domain Names

Domain names regulation is characterized by great diversity. Three out of 10 countries have clear domain names legislation and four have some form of regulation in place. Antigua and Barbuda's Telecommunications Bill from 2007, which would completely reform the current regime, remains in draft form. Jamaica and Trinidad and Tobago have ea.

Table 4 provides the current state of law adoption in the region. Table 5 (in the annex) provides a more detailed state of law adoption in the Caribbean.

Table 4. Overview of the status of e-commerce law harmonization in the Caribbean in December 2016

	Electronic Transactions Law	Consumer Protection	Data Protection and Privacy	Cybercrime and Cybersecurity	Online Content	Domain Names
Antigua and Barbuda	Enacted	Enacted	Enacted	Enacted	Partial	Draft
The Bahamas	Enacted	Enacted	Enacted	Enacted	Partial	Partial
Barbados	Enacted	Enacted	Draft	Enacted	Partial	Enacted
Costa Rica	Enacted	Enacted	Enacted	Partial	None	Partial
Cuba	Draft	None	Partial	Enacted	None	Enacted
El Salvador	Draft	Enacted	Partial	Draft	None	Enacted
Jamaica	Enacted	Enacted	Partial	Enacted	Partial	None
Saint Lucia	Enacted	Partial	Enacted	Enacted	Partial	Partial
Suriname	Draft	Draft	Partial	Partial	None	Partial
Trinidad and Tobago	Enacted	Enacted	Partial	Enacted	Partial	None

Source: UNCTAD, 2017

PART II
REPORTS ON THE LEGAL FRAMEWORK IN THE PARTNER STATES

A. ANTIGUA AND BARBUDA

Economy	2015
GDP, current USD (state as millions - is $1.4 billion)	1,309
GDP per capita, current USD	14,253
Real GDP growth, y-on-y, %	4.10

Merchandise Trade	2015
Merchandise exports, millions USD	55
Merchandise imports, millions USD	457
Merchandise trade balance (millions USD assumed)	-402
Main marchandise exports, %	
Manufactured goods	67
Fuels	23
All food items	8
T exports, millions USD	
Poland	24
Cameroon	6
Suriname	6
Nigeria	4
Dominican Republic	2

Trade in Services	2015
Services exports, millions USD	491
Services imports, millions USD	246
Services trade balance (millions USD assumed)	246
Main services exports, %	
Travel	63
Transport	23

Financial Flows	2015
ws, millions USD	154.06
ws, millions USD	5.76
Personal remittances, % of GDP	1.66

Demography	2015
Population, millions	0.092
Land area, km^2	440

ICT	2014
Share of ICT goods, % total exports	2.23
Share of ICT goods, % total imports	3.83

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

ANTIGUA AND BARBUDA

The legal system in Antigua and Barbuda is based on statutes and English common law. The constitution dates back to 1981, when independence was achieved. In terms of electronic commerce, it has been involved in a long-running dispute with the US over cross-border Internet gambling, which Antigua has been pursuing before the World Trade Organization[3].

1.1 E-transactions law

The Electronic Transactions Act 2006 ('ETA')[4] contains nine substantive parts, addressing the 'Legal requirements respecting electronic records' (Part II); 'E-government services' (Part III); 'Formation and validity of contract' (Part IV); 'Communication of electronic records' (Part V); 'Electronic signatures' (Part VI); 'Information security service providers' (Part VII); 'Liability of intermediaries and service providers' (Part VIII) and 'Miscellaneous' (Part IX).

In terms of Parts I to V, the ETA is based closely on both the UNCITRAL Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001).[5]

Under the ETA, electronic records and signatures shall not be denied admissibility in legal proceedings solely on the basis that they are in electronic form (s. 11). This has been supplemented by the Evidence (Special Provisions) Act 2009 (Cap. 296), which reforms and repeals many of the existing provisions of the Evidence Act (Cap. 155) dating back to 1876. The 2009 Act provides for the admissibility of 'business records', whether electronic or otherwise, 'made in the usual and ordinary course of business' (s. 40). In relation to electronic documents, the burden of proving authenticity resides with the person seeking to adduce the document. The 2009 Act then two evidential 'presumptions' relating to the integrity of electronic documents (s. 43) and secure electronic signatures (s. 44). The former would be applicable to the 'business records' of non-parties, such as an Internet Service Provider; while the latter requires Ministerial regulations, which have not been forthcoming to date. Finally, provision is made for a party to make reference to 'any standard, procedure, usage or practice' followed in relation to electronic documents when determinations of admissibility are made (s. 45). While referencing standards is to be welcomed,[6] the provision seems to confuse admissibility with authentication.

1.2 Consumer protection

Existing consumer protection laws, such as the Consumer Protection and Safety Act 1988 (Cap. 97) and the Unfair Contract Terms Act 1987 (Cap. 451), are currently being reviewed to take into account electronic commerce.

Under Part IX of the ETA, there is one provision directed at consumer protection issues. An online retailer is required to provide certain information to consumers, including their principal geographic address, a description of the goods or services being offered and terms associated with the transaction. The consumer should be able to maintain an adequate record of such information, which would include making a local copy.

The Electronic Funds Transfer Crimes Act 2007 (Cap. 292) contains a provision limiting the liability of a cardholder for the misuse of his payment card (s. 21), subject to various conditions. Such a provision can be very important in terms of giving consumers onic commerce.

1.3 Data protection and privacy

The Constitution recognizes a generalized right to privacy, as well as protection from arbitrary search or entry of a person or his property.[7]

The Data Protection Act 2013 ('DPA') has been adopted, which was closely based on Grenada's Privacy and Data Protection Law and broadly r
the current EU data protection regime. It is divided into four main parts: obliging data users to comply with six data protection principles; granting rights to data subjects; detailing certain exemptions and granting powers, duties and functions upon the Information Commissioner, a post established under the Freedom of Information Act 2004 ('FOIA').[8]

Under the ECA, there is an offence of 'violation of privacy', which attracts a penalty of up to 5 years imprisonment (s. 8). The offence is committed when a person 'captures, publishes or transmits the image of a private area of a person' without consent. This would appear to be designed to criminalize the use of cameras, such as on a mobile phone, to capture images.

The FOIA includes an exemption from the general right of access, where it would involve as "unreasonable disclosure of personal information about a third party who is a natural person" (s. 26(1)), unless the person has consented, the person making the request is a guardian or next of kin, the person has been dead

for over 20 years or it relates to a public in execution of his duties.

1.4 Cybercrime and cybersecurity

Antigua and Barbuda has a number of laws applicable to various forms of cybercrime, primarily the Electronic Crimes Act 2013 (Cap. 298) ('ECA'), which expressly prevails over other criminal provisions. The ECA addresses substantive criminal offences as well as matters of criminal procedure relating to investigations.

Concerning substantive offences, the ECA includes provisions on computer-related cybercrimes, such as fraud and forgery; computer integrity cybercrimes, such as unauthorised access and interference, and content-related, such as child sexual abuse images and offensive messages. In 2006, a Computer Misuse Bill was proposed, which would have been limited primarily to computer integrity offences.[9] The ECA also criminalizes the 'misuse of encryption', where the use of encryption is designed to facilitate the commission of an offence, such as extortion, or to hide incriminating evidence. The ECA provides that its offences are extraditable.

Additional substantive offences are contained in the Electronic Funds Transfer Crimes Act 2007 and the Telecommunications (Prevention and Prohibition of Unauthorised Use and Services) Act 1994 (Cap. 810). The former addresses theft, fraud and forgery, both physical and electronic. The latter is designed to prevent certain usage, such as 'call-back' services, which are considered to threaten the integrity of domestic communication networks and their revenues from inter [10]

In terms of criminal procedure, the ECA grants powers to law enforcement agencies designed to facilitate the investigation and prosecution of cybercrimes.

Overall, the legal framework would seem generally harmonized with the leading international instrument in the the Council of Europe Convention on Cybercrime (2001), although the ECA does not address issues of international co-operation.

1.5 Online content

Part VIII of the ETA addresses the 'liability of intermediaries and service providers'. These provisions are based on those contained in the EU Electronic Commerce Directive,[11] offering legal protections to intermediaries that provide 'mere conduit', 'caching' or 'hosting' services in respect of third-party content. It also extends protection to the provision of 'information location tools', which would cover search engine providers, such as Google.

In respect of mere conduit and caching, the immunity appears to extend to all forms of liability, civil and criminal; while for hosting and information location tools, the immunity only extends to liability 'for damages', which would presumably only arise under a civil suit. For hosting, the limitation is also subject to a requirement that the service provider has an agent capable of receiving of of infringement'. Any such is also subject to detailed provisions governing the form it should take, and it is an offence to misrepresent any fact detailed

As under European law, the intermediary or service provider is not obliged to engage in any general monitoring of content processed by its systems, in order to ascertain whether the processing is unlawful. A court or authority may, however, order the provider to monitor in a instance.

The Minister for Telecommunications may establish standards or conduct requirements though secondary regulations. Alternatively, such standards may be developed by representative industry bodies and approved by the Minister. The standard may relate to a range of matters, including the types of customers to whom a service can be provided. Breach of a regulatory standard can result in the provider committing an offence, although it is not clear if such sanctions would be applicable to breaches of an approved industry code. We are not aware of any such regulations having been adopted to date.

1.6 Domain names

The telecommunications sector is currently governed by the Telecommunications Act 1951 (Cap. 423), as implemented by the Telecommunications Division within the Ministry of Telecommunications, Science and Technology.[12] The regime operates through a licensing regime, which includes a licence for 'Internet service providers'. There is the Telecommunications Bill 2007, which would completely reform the current regime, but it has not yet been enacted.[13] Under the Bill, an independent Telecommunications Commission would be responsible for 'managing the allocation of Internet domain names'.[14]

Currently, the task of allocating the .ag top-level domain name (ccTLD) has been assigned to a domain registry managed by a private company, NicAg,[15] and use is governed by private agreement, under the laws of the State of New York in the United States.[16]

B. THE BAHAMAS

Economy	2015
GDP, current USD (state as millions - is $8.5 billion)	8,522
GDP per capita, current USD	21,962
Real GDP growth, y-on-y, %	-1.70

Merchandise Trade	2015
Merchandise exports, millions USD	629
Merchandise imports, millions USD	3,161
Merchandise trade balance, millions USD	-2,533
Main marchandise exports, %	
Manufactured goods	60
Fuels	34
T exports, millions USD	
Côte d'Ivoire	200
United States	122
Poland	65
Dominican Republic	59
Singapore	32

Trade in Services	2015
Services exports, millions USD	2,740
Services imports, millions USD	1,206
Services trade balance, millions USD	1,534
Main services exports, %	
Travel	89.4
Transport	4.0

Financial Flows	2015
ws, millions USD	384.91
ws, millions USD	158.13

Demography	2015
Population, millions	0.388
Land area, km^2	10.010

ICT	2014
Share of ICT goods, % total exports	0.62
Share of ICT goods, % total imports	3.00

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

THE BAHAMAS

In 2003, the Ministry of Finance published a policy statement on 'Electronic Commerce and the Bahamian Digital Agenda'.[17] The Statement proposed the introduction of four bills designed "to build trust in, and provide certainty and predictability for, online transactions", as well as reform of intellectual property rights and facilitation of the provision of online dispute settlement (paras. 30-31). This reform programme was successfully completed.

1.1 E-transactions law

The Electronic Communications and Transactions Act 2006 (Chap. 337A) ('ECT') comprises four substantive parts, Part II addresses the 'Legal recognition and functional equivalency of electronic communications, signatures, contracts and related matters'. It largely r the provisions of the UNCITRAL Model Law on electronic commerce (1996).

Under Part IV, the applicable Minister, who is currently the Minister of Finance, should appoint an 'E-Commerce Advisory Board', but no such body appears to have been established. The Minister has powers to make regulations under the ECT in respect of electronic signatures and the use, import and export of encryption technologies (s. 24(b)).

1.2 Consumer protection

Consumer law in the Bahamas r the of both the EU and US. The Unfair Terms in Consumer Contracts Act 2006 (Chap. 337B), adopted as part of the electronic commerce strategy, is based on EU law; while the Consumer Commission established under the Consumer Protection Act 2006 (Chap. 337C) is largely modeled on the US Federal Trade Commission.

1.3 Data protection and privacy

The of the Data Protection Commissioner[18] was established under the Data Protection (Privacy of Personal Information) Act 2003 (Chap. 324A). The Act is largely based on EU Directive 95/46/EC and the UK's implementing law, the Data Protection Act 1998. The Commissioner has a power to prohibit transfers of personal data out of the Bahamas, unless protected by contract or equivalent statutory protections (s. 17).

1.4 Cybercrime and cybersecurity

The Computer Misuse Act 2003 (Chap. 107A) addresses computer integrity offences, such as unauthorised access, and the use or interception of a computer service. The offences are subject to enhanced penalties where the target is a 'protected computer', which encompasses those used for the security or defence of the Bahamas, public safety, and various critical national infrastructure, such as communications, banking and services, public utilities, transportation or public key infrastructure (s. 9). In the course of criminal proceedings, a compensation order can be made by the court against an offender, to recompense the victim of any misuse (s. 13).

The Act also contains some reforms to criminal procedure. In particular, existing warrant powers of search under the Criminal Procedure Code (Chap. 91, s. 70), can be used to access a computer and to search any data on the computer 'or available to such computer', which would potentially extend to data stored remotely on cloud services. An investigator can also demand access to 'any information, code or technology' that enables access to protected data, such as encrypted folders (s. 16).

1.5 Online content

Part III of the ECT addresses the liability of intermediaries, who are in the following terms:

"means a person including a host who on behalf of another person, sends, receives or stores either temporary or permanently that electronic communication or provides related services with respect to that electronic communication;"

The immunity extends to both civil and criminal liability, where the intermediary has no actual knowledge or is not aware of facts or circumstances from which he 'ought reasonably' to have known (s. 19). Different procedures are applicable to intermediaries depending on whether they gain actual knowledge or just awareness. For the former, the intermediary has to act 'as soon as practicable' and remove the information; for the latter, the obligation is to comply with any applicable code of conduct. In both cases, however, the intermediary must notify the police, and for the latter situation the Minister as well. The reporting obligation is highly unusual, particularly to

a government Minister and especially where it only relates to potential civil liability.

Intermediaries and e-commerce providers[19] are under a general obligation to comply with an approved code of conduct or appointed standard. Failure to comply can give rise to a (s. 21). No such code appears to have been approved to date.

1.6 Domain names

Under the ECT, the Minister may issue regulations governing the .bs ccTLD and the designation of registration authorities (s. 24(c) and (d)). The domain is operated by BSNIC under the sponsorship of the College of the Bahamas.

C. BARBADOS

Economy	2015
GDP, current USD (state as millions - is $4.3 billion)	4,335
GDP per capita, current USD	15,253
Real GDP growth, y-on-y, %	0.80

Merchandise Trade	2015
Merchandise exports, millions USD	483
Merchandise imports, millions USD	1,618
Merchandise trade balance, millions USD	-1,135
Main marchandise exports, %	
Manufactured goods	56
All food items	25
Fuels	15
T partners, exports, millions USD	
Trinidad and Tobago	95
United States	61
Jamaica	36
Saint Lucia	34
Nigeria	21

Trade in Services	2015
Services exports, millions USD	1,481
Services imports, millions USD	701
Services trade balance, millions USD	780
Main services exports, %	
Travel	67.4

Financial Flows	2015
ws, millions USD	254.42
ws, millions USD	85.95
Personal remittances, % of GDP	2.50

Demography	2015
Population, millions	0.284
Land area, km^2	430

ICT	2014
Share of ICT goods, % total exports	0.77
Share of ICT goods, % total imports	5.37

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

BARBADOS

The Barbados legal system is based largely on English common law, with a Constitution and parliamentary legislation since it became self-governing in 1961.

1.1 E-transactions law

Barbados acted quickly to facilitate the take-up and adoption of an Electronic Transactions Law in 2001 ('ETA'). Parts II and III are closely based on the UNCITRAL Model Law on Electronic Commerce (2001) and are also modeled after the UNCITRAL Model Law on Electronic Signatures (2001). In 2014, the ETA was amended, for 'the improvement of the administration of the Act'.[20] One amendment was the insertion of a new provision on 'mistakes in partly automated transactions' (s. 12A), which can be viewed as a consumer protection measure.

Part IV addresses the and accreditation of electronic signatures. The provisions are based on the EU Directive on electronic signatures,[21] and deem an electronic signature with an accredited from an accredited service provider as satisfying the requirements of an electronic signature laid down in section 8 (s. 17). Originally, the provision of services was not subject to prior authorization, although authorization was stated as being a requirement for the purposes of section 8, which recognizes the validity of electronic signatures. Following the 2014 amendment, a licence is mandatory for all service providers, with criminal sanctions for failing to obtain a licence (s. 18(1)). As such, the regime must be considered a approach, since it is based on the use of a public-key infrastructure. The amendments in 2014 were designed, in part, to render the ETA more technology neutral, by making the concepts of 'accredited and service provider' more technology neutral. The 2014 amendment also established a 'Supervisor of Authorities' (s. 18A), removing the oversight function from the Minister.

1.2 Consumer protection

The primary legal instrument protecting consumers is the Consumer Protection Act 2002 (Cap. 326D). Part IV addresses distance selling, which would include Internet-based commerce. It provides for the Minister to adopt regulations, in consultation with the Fair Trading Commission (s. 27),[22] which is a member of the International Consumer Protection and Enforcement Network (ICPEN).[23] The statute contains a non-exclusive list of issues that may be addressed in such regulations, covering the whole transaction process, from advertising and marketing to dispute resolution. To date, however, no such regulations appear to have been issued.

The ETA did not originally address consumer protection issues, but the amendment in 2014 inserted a provision requiring online vendors to provide certain information to purchasers, including about the vendor's identity and about the terms and conditions of the transaction (s. 16A). However, it is not stated what consequences, if any, would from the failure of a vendor to comply with these obligations.

1.3 Data protection and privacy

A right to 'protection of privacy' is enshrined in the Constitution of Barbados (Art. 11).

The ETA contains a provision on the protection of data and privacy. The provision regulates the disclosure of information relating to the 'private affairs of a natural person or to any particular business' in relation to information obtained by virtue of the Act (s. 22). However, the Minister is also granted the power to make general regulations 'prescribing standards for the processing of personal data' (s. s. 22(6)), which could include the establishment of a registration scheme.

A comprehensive Data Protection Bill has been drafted,[24] based on the UK's Data Protection Act 1998, which is itself based on the EU Data Protection Directive (95/46/EC). It currently remains in draft form.

1.4 Cybercrime and cybersecurity

The Computer Misuse Act 2005 ('CMA') covers both substantive criminal law and criminal procedure.[25] In terms of offences, the focus in on conduct designed to undermine the , integrity and availability of computers and networks, as well as the programmes and data they contain. Supplemental offences exist where the target is a 'restricted computer system', which are systems belonging to the entities detailed in the Schedule, as may be amended by the Minister (s. 11). These include government departments, hospitals and the courts. Two content-related cybercrimes are addressed, in relation to both the publishing and possession of 'child pornography'

(s. 13); as well as indecent, obscene, threatening or menacing communications (s. 14), which could be used against so-called Internet 'trolls'. There is a very similar provision in the Telecommunications Act 2001 (Cap. 282B), at s. 81.

Part III of the CMA provides law enforcement with new powers to help investigate computer crimes. It enables, for example, a search to be extended to "any programme or data held in or available to such computer", which recognizes the connected nature of modern computing systems. The power to obtain access to encrypted data is also granted to law enforcement (s. 15(2)(d)), as well as requiring persons to assist in such a process or face committing an offence (s. 16(1)(d)). Under the ETA, the Minister may make regulations governing the use, import or export of encryption programmes (s. 21).

In August 2013, the Government signed an agreement with the ITU to establish a national Computer Incident Response Team (CIRT).[26] However, at the time of drafting this study, the CIRT is still in the process of being established.

1.5 Online content

The ETA contains two provisions addressing the liability of an 'intermediary' for third-party content. The immunity extends to both civil and criminal liability, where the intermediary neither has 'actual knowledge' not is aware of any facts or circumstances from which he ought to have reasonably known (s. 23(1)(a)). Once knowledgeable or aware, the intermediary must, 'as soon as practicable', remove the information and notify the Minister or appropriate law enforcement agency. The Minister may then direct the intermediary to take certain actions, and the intermediary is immune from liability for any such directed actions (s. 24).

1.6 Domain names

The Government of Barbados, through the Telecommunications Unit,[27] took over the administration of the ccTLD '.bb' from 18 February 2008. The administration of the domain is governed by a policy issued by the Minister under powers granted in the Telecommunications Act 2001.[28]

D. COSTA RICA

Economy	2015
GDP, current USD (state as millions - is $52.2 billion)	52,159
GDP per capita, current USD	10,849
Real GDP growth, y-on-y, %	3.70

Merchandise Trade	2015
Merchandise exports, millions USD	9,624
Merchandise imports, millions USD	15,503
Merchandise trade balance, millions USD	-5,879
Main marchandise exports, %	
Manufactured goods	55
All food items	40
T partners, exports, millions USD	
United States	3,354
China	486
Guatemala	425
Nicaragua	393
Mexico	381

Trade in Services	2015
Services exports, millions USD	7,706
Services imports, millions USD	2,667
Services trade balance, millions USD	5,039
Main services exports, %	
Travel	42.5
Transport	3.6

Financial Flows	2015
ws, millions USD	2,849.60
ws, millions USD	141.15
Personal remittances, % of GDP	1.06

Demography	2015
Population, millions	4.808
Land area, km^2	51.060

ICT	2010
Share of ICT goods, % total exports	19.91
Share of ICT goods, % total imports	17.72
Share of workforce involved in the ICT sector, %	4.70

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

COSTA RICA

Costa Rica is a civil law country with a Civil Code based on the French Napoleonic Code as adopted in Spain. The Civil Code dates back to 1887, while the Constitution dates from 1949.

1.1 E-transactions law

In 2005, Costa Rica adopted the Ley de Certificados, Firmas Digitales y Documentos Electrónicos,[29] which is applicable to both private and public sector transactions, but specifically authorizes the use of electronic documents, digital signature and certificates by the public sector (Art. 1). The law lays down a general principle of 'functional equivalence' between paper and electronic (Art. 3). It supplements the Commercial Code (Act No. 3284) governing commercial transactions and the Civil Code (Law No. 63) governing contractual formalities. The law is based on UNCITRAL's Model Law on Electronic Signatures.

Section III of the law gives detailed attention to the use of 'digital signatures' and 'certificates', granting beneficial legal presumptions to their use and establishing a Directorate of Digital Signature Certifiers Certification under the Ministry of Science and Technology ('MICIT').[30] Supplemental regulations have been adopted by the MICIT,[31] which set out the hierarchy and functions of participants, such as the 'Root Certifier', as well as detailing technical guidelines that certifiers are obliged to comply with.

With regard to procurement by the public sector, the Public Procurement Act (Act No. 7494 of 1995) recognizes the use of electronic communications in the procurement process, provided procedures are place to ensure the integrity of message receipt and content. In the field of public administration, guidelines ? require public sector institutions to implement technical and financial measures to enable citizens to obtain information, ask questions, make requests, express their consent and commitment, make payments and ? transactions and oppose resolutions and administrative acts by using electronic means.[32]

A further law on electronic commerce has been proposed, but it has not been adopted by the legislature.[33]

1.2 Consumer protection

In the area of consumer protection, the 'Law on Promotion of Competition and Effective Consumer Protection' (Law No. 7472 of 1994) incorporates the basic principles contained in Resolution 39/248 on Guidelines for Consumer Protection, approved by the United Nations General Assembly.[34] Amongst other things, the law regulates the obligations of traders to provide consumers with adequate information. It also establishes administrative and judicial measures against misleading advertising, unfair terms and practices, unfair business methods or restrictions on freedom of choice.

Under the 'Law on Promotion of Competition and Effective Consumer Protection',[35] the concept of 'broadcast medium' was extended to include email and other electronic means of communicating advertising material. Similarly, consumers were given a right of withdrawal, which can be exercised by sending a message within eight days from the conclusion of a sale.

1.3 Data protection and privacy

In addition to constitutional protections, data protection is governed by Ley Protección de la Persona frente al Tratamiento de sus Datos Personales ('Law of Protection of the Person in the Processing of His Personal Data');[36] as well as the Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales ('Regulations of the Law of Protection of the Person in the Processing of His Personal Data').[37] The regime is in accordance with the 'Guidelines for the Harmonization of Data Protection in the Ibero-American Community' issued by the Latin American Network of Protection of Personal Data.[38] It is applicable to both manual and electronic data processing carried out by public and private sector entities.

In March 2012, the authority established to implement these laws is the Agencia de Protección de Datos de los Habitants ('PRODHAB').[39] Its work is funded through registration fees paid by database operators, both public and private.

Under the Act, organizations have to register a 'Performance Protocol' with PRODHAB that effectively details how personal data will be handled in a secure manner. In terms of data retention, the general rule is that personal data should be deleted when it is no

longer necessary for the purpose of the processing, but there is also a maximum retention period of 10 years, unless otherwise required by law or the data is anonymized. Express consent is required for most types of processing, including international transfers. Security br equired.

1.4 Cybercrime and cybersecurity

The Penal Code was amended in 2001 and 2012 to introduce a number of offences relating to computer crime.[40] With regard to computer integrity, there is an offence of 'violation of electronic communications' (Art. 196 bis), which would seem to cover a range of conduct without the consent of the communicating parties, including access, interference, and interception. In addition, data alteration and computer sabotage are offences (Art. 229 bis). This establishes an offence where a person without authorization deletes, or disables a computer or the data held on it. The penalty is expanded [or extended] from four to eight years imprisonment where the computer, database or system contains 'public data'. For computer-related crime, an offence of computer fraud has been inserted (Art. 217 bis), which covers the processing of data by a programme, using false or incomplete data or other related actions.

1.5 Online content

No information available.

1.6 Domain names

On 10 September 1990, the International Assigned Numbers Authority (IANA) issued the .cr top-level domain to Costa Rica, under the administration of NIC Costa Rica, a specialized unit of the National Academy of Sciences.[41]

The Domain Deletion Policy states that in the event of a dispute over a domain name registered under the .cr, the NIC will proceed to remove the domain name until a judgment of a national court or abroad is issued. However, the procedure does not apply to ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP).

E. CUBA

Economy	2015
GDP, current USD (state as millions - is $90.3 billion)	90,311
GDP per capita, current USD	7,929
Real GDP growth, y-on-y, %	4.30

Merchandise Trade	2015
Merchandise exports, millions USD	4,400
Merchandise imports, millions USD	15,090
Merchandise trade balance, millions USD	-10,690
Main marchandise exports, %	
Manufactured goods	38
All food items	30
Ores and metal	11
Fuels	19
Top partners, exports, millions USD	
Venezuela	1,047
Canada	671
China	611
Spain	219
Netherlands	188

Trade in Services	2015
Services exports, millions USD	10,551
Services imports, millions USD	2,125
Services trade balance, millions USD	8,425
Main services exports, %	
Travel	22.9

Demography	2015
Population, millions	11.390
Land area, km^2	106.449

ICT	2005
Share of ICT goods, % total exports	0.86
Share of ICT goods, % total imports	2.64

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

CUBA

In 1999, a National Commission for Electronic Commerce was established, with objective of proposing policy recommendations to facilitate the development of electronic commerce. In 2001, a resolution called upon the national telecommunications operator, Empresa de Telecomunicaciones de Cuba SA (ETECSA), to prioritize electronic commerce solutions.[42] Various legal and regulatory measures and amendments have been subsequently passed, especially concerning cybersecurity.

1.1 E-transactions law

Regulatory proposals from the Ministry of Justice are currently under review and include a decree on 'General rules for the practice of electronic commerce' ('eCommerce Decree'). The draft incorporates provisions regulating the transmission and reception of data messages, business carried out electronically (authorized by the Ministry of the Interior), protection of personal data, activities of and registration authorities and of entities that carry out and registration functions, as well as registries (under the auspices of the Ministry of Justice).

To facilitate payments relating to electronic commerce, the Central Bank of Cuba issued Resolution 61/2002, which lays down rules for the collection and payment of charges relating to e-commerce transactions.[43]

1.2 Consumer protection

In the of consumer protection, Cuba does not have a law on the subject, though related issues are addressed in the context of the 'System of Consumer Protection', in force since 2001, which applies to all retailers.

The draft eCommerce Decree contains rules designed to protect consumers, by imposing transparency obligations on vendors, including costs and any additional charges.

1.3 Data protection and privacy

Cuba's Constitution dates from 1976, with the most recent amendments in 2002. While the Constitution recognizes a right to communications privacy (Art. 57), no other personal data rights are recognized.

1.4 Cybercrime and cybersecurity

The Ministry of Communications (MINCOM), formerly the Ministry of Informatics and Communications (MIC), has responsibility for cybersecurity issues. In 2007, it adopted a resolution on 'Safety Regulations for Information Technology', addressing the , integrity and availability of information processed by computers and data networks".[44] Under the resolution, an for Secure Networking was established within the Ministry, which has since been renamed the Centro de Seguridad del Ciberespacio.[45] In addition, the Council of Ministers has issued 'Guidelines for Improving the Security of Information Technologies'.[46]

The Regulations are applicable to all users, whether public sector, private sector, associations or individuals (Art. 3). It imposes a general obligation on users to implement security measures, based on the nature of the material and potential risks. The resolution provides for inspectors who can carry out security audits, with or without notice (Art. 98(a)). Each public agency has to appoint a person to take responsibility for managing information security procedures (Art. 9 and 10), while all users are responsible for any improper use, including notifying of any suspected breaches (Art 11, 12 and 24). The Regulations detail measures that must be taken to protect all aspect of cybersecurity, from physical and environmental measures to data backup.

The Penal Code (Act No. 62 of 1987, as amended by Act No. 97 of 1999) contains a number of offences relevant to cybercrime; for example, Article 289 criminalizes unauthorized interception of communications. However, there are no offences in respect of conduct targeting the , integrity and availability of computers, networks or the programmes and data held on them. There is an ongoing project to renew the Penal Code, 'Proyecto el nuevo Código Penal', but no further details are available.

1.5 Online content

No information available.

1.6 Domain names

The domain name system in Cuba is the responsibility of MINCOM, in accordance with Resolutions 72/2013 on the 'Regulation of Domain Names', 103/2011 on the System of Internationalized Domain Names and 71/2015 on 'Regulations for the Management of Resources: IP Numbering'.[47] However, by virtue of Resolution 280/2015, the management of .cu is the responsibility of the Cuban Network Information Center ('CUBANIC'), which operates under the Ministry of Science, Technology and the Environment.[48]

F. EL SALVADOR

Economy	2015
GDP, current USD (state as millions - is $25.6 billion)	25,605
GDP per capita, current USD	4,179
Real GDP growth, y-on-y, %	2.50

Merchandise Trade	2015
Merchandise exports, millions USD	5,485
Merchandise imports, millions USD	10,416
Merchandise trade balance, millions USD	-4,931
Main marchandise exports, %	
Manufactured goods	76
All food items	20
T exports, millions USD	
United States	2,518
Guatemala	782
Honduras	650
Nicaragua	350
Costa Rica	245

Trade in Services	2015
Services exports, millions USD	2,324
Services imports, millions USD	1,545
Services trade balance, millions USD	779
Main services exports, %	
Travel	35.2
Transport	21.0

Financial Flows	2015
ws, millions USD	428.71
ws, millions USD	-0.09
Personal remittances, % of GDP	16.74

Demography	2015
Population, millions	16.127
Land area, km^2	20,720

ICT	2014
Share of ICT goods, % total exports	0.39
Share of ICT goods, % total imports	5.16

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

EL SALVADOR

El Salvador does not appear to have a national strategy for e-commerce, although it participates in the project of the Mesoamerican Information Highway (AMI).[49] Among the major bills that are under review by the Legislative Assembly are draft laws on electronic commerce, trade documents, digital signatures and cybercrime.

1.1 E-transactions law

A draft law was published in March 2001, Ley de Comercio Electronico y Comunicaciones, but has not ogressed since then.

At a procedural level, the Civil and Commercial Procedure Code[50] recognizes the validity of electronically stored data, including magnetic media and computer-derived information, as being admissible as evidence and having probative value in legal proceedings.

In the commercial and area, there are several provisions that recognize functional equivalence between paper and electronic documents, as well as handwritten and digital signatures. The Banking Act 1999[51] and the Law on Electronic Annotations Securities Account 2002,[52] recognize the legal validity of electronic transactions and the use of electronic signatures.

For its part, the Banking Act regulates the function of intermediation and other operations performed by banks under the supervision of the Central Reserve Bank of El Salvador and the Superintendent of the Financial System. It gives validity to evidence contained in systems logs, as well as printouts of electronic records of transactions. It also imposes an obligation of banks to accept electronic instructions for the operations of debit or credit transactions.

The Law on Electronic Annotations Securities Account recognizes the validity of electronic transaction mechanisms. It establishes that electronic book entry securities represent valid securities, included in an electronic register rather than a document. It also recognizes that dematerialized securities have value and that representation through electronic book entry is mandatory for publicly traded securities. It empowers share issuers to operate an electronic register of shareholders in place of Register of Shareholders.

The Customs Act represents an important advance for electronic transactions, by incorporating measures in accordance with the Regulations of the Central American Uniform Customs Code and DR-CAFTA, and contains some provisions that r the UNCITRAL Model Law on Signatures (2001).[53] It authorizes the electronic transmission of goods declarations, or of origin, cargo manifests, bills of lading and other documents required for foreign trade operations. It also authorizes the payment of customs tax obligations by electronic funds transfer. To ensure the authenticity, and integrity of information exchanged between business and customs systems, and to prevent subsequent repudiation, the Act provides for digital of information, by third-party service providers. Each authorized user will have a unique key pair and corresponding keys, which are digital signatures that represents the equivalent of the handwritten signature.

1.2 Consumer protection

Under the Constitution of El Salvador, the state has an obligation to "defend the interests of consumers" (Art. 101). Based on this constitutional provision, the legislature adopted the Consumer Protection Act 2005 (Decree No. 776). Among the consumer rights laid down in the law are rights to receive complete, precise, accurate, clear and timely information on the characteristics of products and services; to receive information about the risks and conditions of any contract; a prohibition on misleading or false advertising, and prohibitions on unfair practices and terms. In January 2013, the Act was amended to include a right to withdraw without liability from a 'distance contract', including by electronic means, for consumers for up to eight days following its conclusion.[54]

1.3 Data protection and privacy

A right to privacy is guaranteed under Article 2 of the Constitution. It was amended in 2010 by a 'Special law on the interception of telecommunications' for law enforcement purposes.[55]

There are also sectoral rules protecting data. Various measures to protect a person's name against misuse are established by the Law of Natural Person Name (1990). The Consumer Protection Act includes measures prohibiting the disclosure of personal and consumer credit information among suppliers or through entities specialized in the provision of information, without proper authorization from the consumer. It imposes obligations on entities

specialized in providing information services, which are obliged to allow consumers access to their data and to apply to update, modify and delete it, free of charge. The entities also have an obligation to correct false, outdated or inaccurate data within a period of ten days from receipt of a request.

In 2011, a law regulating the use of information services on consumers credit history was adopted.[56] The Act aims to protect the right to honor, personal and family privacy and image with respect to issues of reliability, truthfulness, updating and good management of the credit history of consumers. It regulates the activities of persons authorized to operate as credit information agencies.

In the customs area, the Customs Act establishes an obligation to keep secret the personal data of those who have used digital signatures and messaging. It also provides that such personal data may only be used for purposes other than those covered by the Act, where the owner of the data expressly consents in writing to a different purpose.

1.4 Cybercrime and cybersecurity

While neither the Criminal Code (1997)[57] nor the Criminal Procedure Code (2009)[58] refers to computer crime or data messages, their provisions could be applicable in a particular scenario, depending on judicial sentiment towards cases involving computers, programs and data.

A draft law on computer and cybercrime was published in April 2015, Ley Especial Contra Los Delitos Informaticos y Conexos. It includes offences relating to the , integrity and availability of computer systems, programmes and data, as well as content-related crimes, such as an offence of 'dissemination of damaging information' (Art. 24). The latter has generated concerns that it could be used to suppress freedom of expression on the Internet, such as social networking sites,[59] although the Penal Code contains a defence for political, literary and other forms of criticisms (Art. 191).

The Special Law Against Acts of Terrorism (2006)[60] includes some computer crimes. It is an offence to facilitate the commission of any offense under the Act in question using equipment, means, programs, networks or any other computer application to intercept, interfere with, divert, alter, damage, disable or destroy data information, electronic documents, computer media, programs or information systems and communications or telecommunications, utilities, social, administrative, emergency or national security, national, international or foreign entities. It is also an offence to possess, distribute or sell programs capable of causing the mischiefs outlined above.

The Special Law to Sanction Customs Violations (2001)[61] the following computer crimes, which are punishable with imprisonment from three to years: (a) access without authorization and by any means, to computer systems used by the Directorate General of Customs Revenue; (b) seizure, copying, destruction, disabling, altering, supplying, transferring or being in possession, without authorization of the customs authority, of any computer program or database designed by or for the authority in the exercise of their monitoring services; (c) material damage to equipment components, machines or accessories that support the operation of computer or communications systems, designed for operations of the Directorate General; (d) facilitate the unauthorized use of assigned codes and passwords, and (e) interfering with a computer or communications system to prevent the exercise of control over that system (Article 24).

1.5 Online content

No information available.

1.6 Domain names

The Law on Trademarks and Other Distinctive Signs (Decree No. 868, 2006)[62] establishes requirements and terms for the protection of trademarks, trade names, appellations of origin and other distinguishing marks. In cases of domain name piracy, the law provides that the administrator of the ccTLD (.sv) must have procedures for dispute resolution based on the principles set out in ICANN'S Uniform Dispute Resolution Policy.[63] It must also provide online public access to a reliable database and accurate contact information for domain name registrants, while respecting the privacy of registrants (s. 113-A).

In this regard, the Association SVNet (NIC-El Salvador)[64] is responsible for issuing and updating policies for the operation of the .sv top-level domain, and has incorporated the UDRP into its regulations. It also recognizes the Center for Mediation and Arbitration of the American Chamber of Commerce (AMCHAM).

G. JAMAICA

Economy	2015
GDP, current USD (state as millions - is $13.8 billion)	13,812
GDP per capita, current USD	4,945
Real GDP growth, y-on-y, %	0.80

Merchandise Trade	2015
Merchandise exports, millions USD	1,261
Merchandise imports, millions USD	4,862
Merchandise trade balance, millions USD	-3,601
Main marchandise exports, %	
Ores and metals	57
All food items	19
Fuels	16
Manufactured goods	8
T exports, millions USD	
United States	467
Canada	182
Netherlands	110
Iceland	99
Russian Federation	88

Trade in Services	2015
Services exports, millions USD	2,943
Services imports, millions USD	2,137
Services trade balance, millions USD	806
Main services exports, %	
Travel	80.8
Transport	6.3

Financial Flows	2015
ws, millions USD	794.48
ws, millions USD	4.39
Personal remittances, % of GDP	17.09

Demography	2015
Population, millions	2.793
Land area, km^2	10.830

ICT	2014
Share of ICT goods, % total exports	0.29
Share of ICT goods, % total imports	3.65

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

JAMAICA

The legal system of Jamaica is based on English common law. Its constitution dates from 1962.

In 2003, the Ministry of Commerce, Science and Technology in Jamaica published a policy on 'Electronic Transactions', which explicitly recognized the role played by an appropriate legal framework in terms of protecting Jamaicans, giving persons to do business in Jamaica and conforming with international best practice.[65] Subsequently, electronic commerce formed part of the Government's National Information and Communications Technology Strategy (2007-2012), entitled 'E-Powering Jamaica'.[66]

1.1 E-transactions law

Jamaica has an Electronic Transactions Act (Act 15 of 2006) ('ETA'). Part II addresses form requirements and is largely based on UNCITRAL's Model Law on Electronic Commerce (1996). It also includes a provision enabling the Minister to issue regulations to facilitate electronic payments.

Part III regulates the use of electronic signatures, including the provision of services. Part V establishes a Certifying Authority to provide services to, and regulate the provision of services by, service providers. This role was to be given to the Trade Board, although it is not apparent that it currently carries out this role.[67] Further Ministerial regulations may be made concerning the requirements for an 'encrypted signature', the use, (?) import and export of encryption devices, and It is based on UNCITRAL's Model Law on Electronic Signatures (2001).

1.2 Consumer protection

The primary legislative instruments are the Trade Act 1955 and the Consumer Protection Act (Act 9 of 2005). The Act establishes a Consumer Affairs Commission.[68]

Part IV of the ETA imposes obligations on those supplying goods, services or facilities through electronic transactions, whether based in Jamaica or to persons in Jamaica (s. 26(2)(b)). The concept of a 'consumer' includes commercial undertakings that purchase consumer goods. Suppliers have obligations to make available certain information to the consumer (s. 27 and Second Schedule), as well as an opportunity to review a transaction, correct errors, withdraw from the transaction prior to placing the order, and access and archive an electronic copy of the order, including the total costs. The supplier is also required to use a payment system that is secure' or be liable for any damages suffered by a consumer (s. 27(5) and (6)). A 'cooling-off' period is given to consumers, subject to certain exceptions (s. 28). In an effort to control 'spam' (or unsolicited commercial communications), the ETA establishes a number of offences (s. 29). These provisions largely r the EU Distance Selling Directive (1997), the main provisions of which have subsequently been incorporated into the Consumer Rights Directive.[69]

There are sectoral consumer protection rules for the telecommunications sector, under Part VII of the Telecommunications Act (Act 1 of 2000)('TA').

1.3 Data protection and privacy

Under its constitution, Jamaica protects persons from search or entry without authority (Section 19). Jamaica has had a Data Protection Bill since 2012, but no progress has been made towards adoption.

The ETA purportedly provides protection to 'personal information', which includes information about an individual and provides a non-exclusive list of categories of personal data, from so-called 'sensitive data' relating to race, health and religious views, to information about transactions. Rather strangely, however, the ETA does not provide any general protection against the processing of such information, only a narrow right to request the source of any personal information processed by a person sending an unsolicited commercial communication (s. 29(1)(b)); as well as a right to be informed about the security and privacy policy of the supplier (Second Schedule).

Under the TA, every carrier and service provider is required to maintain as secret and all information "regarding the type, location, use, destination, quantity, and technical of services used by their customers" (s. 47). This obligation is subject to exceptions only for law enforcement purposes or with the written consent of the customer.

1.4 Cybercrime and cybersecurity

A Cybercrimes Act was adopted in 2010. Part II addresses computer integrity offences and is partly based on the UK's Computer Misuse Act 1990. Part III deals with investigations. Or did you mean to say more?

In addition, the Interception of Communications Act (Act 5 of 2002) criminalizes acts of interception through a general prohibition (s. 3); while specifying certain lawful grounds for interception and providing for a judicial warranting scheme for interception in the course of a criminal investigation or on national security grounds.

1.5 Online content

The ETA contains an intermediary liability provision, which grants immunity from civil and criminal liability in circumstances, unless the intermediary has 'actual knowledge' or knowledge of facts and circumstances from which they 'ought reasonably to have known' (s. 25). Intermediaries are granted an express protection from any obligation to monitor, although not where required by law, court order, ministerial direction or under a contractual obligation.

1.6 Domain names

The .jm domain is handled by MITS at the University of the West Indies.

H. SAINT LUCIA

Economy	2015
GDP, current USD (state as millions - is $1.4 billion)	1,436
GDP per capita, current USD	7,761
Real GDP growth, y-on-y, %	2.40

Merchandise Trade	2015
Merchandise exports, millions USD	179
Merchandise imports, millions USD	570
Merchandise trade balance, millions USD	-391
Main marchandise exports, %	
Manufactured goods	33
All food items	33
Fuels	32
T exports, millions USD	
United States	38
United Kingdom	35
Trinidad and Tobago	16
Korea, Republic of	15
France	13

Trade in Services	2015
Services exports, millions USD	448
Services imports, millions USD	183
Services trade balance, millions USD	265
Main services exports, %	
Travel	87.1
Transport	3.3

Financial Flows	2015
ws, millions USD	95.03
ws, millions USD	2.53
Personal remittances, % of GDP	2.10

Demography	2015
Population, millions (or 185 in 000s)	0.185
Land area, km^2	610

ICT	2014
Share of ICT goods, % total exports	11.65
Share of ICT goods, % total imports	4.50

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

SAINT LUCIA

Saint Lucia's legal system is based on the English common law. The constitution dates from 1978.

1.1 E-transactions law

An Electronic Transactions Act was adopted in 2011 (No. 16 of 2011) ('ETA'), based on UNCITRAL's model laws on electronic commerce and electronic signature. It comprises six parts. Part 2 contains a general provision stating that information "must not be denied legal effect solely" because it is in electronic form or is referred to in an electronic communication (s. 5); while the remaining provisions detail the time and date of dispatch and receipt of an electronic communication. Part 3 details how legal requirements of form, such as recording information 'in writing', apply to electronic transactions. While containing a general facilitative provision, it then goes on to detail the numerous types of requirements that may create uncertainties. Part 4 addresses the validity of electronic contracts.

1.2 Consumer protection

Part 5 provides consumer protection measures designed to supplement existing consumer protection laws. Suppliers are required to make available to consumers a wide range of information, as well as provide an opportunity to review, correct and withdraw from electronic transactions. A failure to meet these requirements gives a consumer the right to cancel the transaction up to 14 days after receiving the goods or services (s. 45(3)). This right is applicable to all forms of transactions, without exception, which could encourage abusive behaviour by consumers in respect of certain types of transactions, especially services that have already been consumed or could be easily copied. A comprehensive seven-day cooling-off period is provided for all transactions, but subject to a range of exemptions and limitations designed to limit opportunities for abuse, such as clearly personalized products.

Suppliers have an obligation to utilize a 'sufficiently secure' payment system, based on the state of technological development and nature of the transaction, and would be liable for any damage suffered by a consumer from a failure to meet this obligation.

1.3 Data protection and privacy

Saint Lucia's current constitution dates from 2006 and contains a broad right to protection for privacy (Chap. 1(1)).

The Data Protection Act (No. 11 of 2011) is based partly on the UK's Data Protection Act 1998. It establishes the of the Data Protection Commissioner, but the appointment has not yet been made and therefore the Act has not yet come into force. In 2015, the Act was amended (No. 2 of 2015) to introduce freedom of information provisions.

Telecommunications providers have an obligation to ensure that communications cannot be intercepted except when authorized by the recipient or under a court order authorizing law enforcement to engage in such activities.[70] However, telecommunication providers are also obliged to report any transmission that "appears likely to threaten the national security or is contrary to public order" (r. 9(2)). It is not clear in what circumstances a provider would become aware that the content of a particular transmission is likely to contain such content unless it engages in some sort of on-going monitoring of which the former provision prohibits.

The 'personal information' or 'proprietary network information'[71] of subscribers must be protected by telecommunication providers, especially against the unauthorized actions of employees or (Part IV). However, such obligations do not appear to extend to any users of the services who are not subscribers,

1.4 Cybercrime and cybersecurity

St Lucia's Criminal Code dates from 2005 (Act 9 of 2004). Having been recently updated, it contains a offence of computer fraud (s. 267), which criminalizes a person who, 'with intent to defraud or deceive', either data or programmes or causes an unauthorized to the contents of a computer or network. The maximum penalty is 15 years imprisonment. Content-related offences, in relation to obscenity and indecency, also expressly extend to data held on a computer.

The code also contains provisions on criminal procedure, at Chapter 3. With regard to an authorized search, an is entitled search any computer in the building or place, as well as any data "available

to the computer system" (s. 624(2)(a)), which would enable access to remote computers networked to the computer in the building or place, subject to any jurisdictional limitations that may be implied over the exercise of such a power. The magistrate granting the warrant may also permit an to use techniques, including an 'electronic device', designed to observe a person engaged in an activity for which he has "a reasonable expectation of privacy", subject to any such conditions as may be considered appropriate by the magistrate to protect the privacy of the person or any other person, i.e. collateral interference (s. 624(7)).

The Computer Misuse Act (No 12 of 2011) ('CMA') is divided in two main parts. The establishes a range of computer integrity, content-related and computer-related offences. It includes an offence of 'electronic fraud', which differs from the Criminal Code 'computer fraud' offence and may therefore give rise to uncertainties for prosecutors. The computer-integrity offences are partly based on the provisions of the UK Computer Misuse Act 1990, as well as incorporating the US concept of 'protected computer systems', which means the systems operating key public infrastructure that are subject to enhanced penalties for deterrence purposes.

The second part of the CMA addresses the investigative power of law enforcement agencies (LEAs) to "facilitate the gathering and use of electronic evidence" (s. 3(c)). These provisions r the provisions of the Council of Europe Cybercrime Convention (2001). This includes powers to demand access to encrypted systems and data, which may be in the possession of a suspect or, more often, under the control of a service provider.

Telecommunication providers have reporting obligations concerning the security of their systems and the data they process.[72] First, they must report to the National Telecommunications Regulatory Commission (NTRC) on a quarterly basis any suspected interceptions or breach of security policies and procedures. Second, they have a breach obligation where there has been unauthorized access to a subscriber's 'personal information' or 'proprietary network information'.

Saint Lucia has enacted the Electronic Crimes Act 2009, which is not yet in force. It provides for the prevention and punishment of electronic crimes.

1.5 Online content

Part 6 of the ETA protects intermediaries and Internet Service Providers from liability when providing conduit for third party content. Ministerial regulations should be adopted detailing the procedures to be expeditiously followed once the unlawful nature of the information comes to the attention or notice of the provider. No such regulations appear to have yet been promulgated.

1.6 Domain names

Under the Telecommunications Act (No. 27 of 2000), the National Telecommunications Regulatory Commission ('NTRC')[73] has been designated as being responsible for the "registration and management of Internet domain names" (s. 53). The Minister may issue regulations on such matters (s. 74(2)(x)), but none have been issued to date. NTRC has delegated the task of managing the ccTLD .lc domain name to egistry.[74]

The NTRC is part of the Eastern Caribbean Telecommunications Authority ('ECTEL'),[75] which is currently consulting on a new Electronic Communications Bill, which would replace the current legislation with a broader regulatory framework.[76] However, the NTRC would remain responsible for the management of domain names.

I. SURINAME

Economy	2015
GDP, current USD (state as millions - is $5.3 billion	5,271
GDP per capita, current USD	9,708
Real GDP growth, y-on-y, %	-2.00

Merchandise Trade	2015
Merchandise exports, millions USD	1,666
Merchandise imports, millions USD	1,973
Merchandise trade balance, millions USD	-307
Main marchandise exports, %	
Ores and metals	16
All food items	10
Fuels	10
Manufactured goods	5
T exports, millions USD	
United Arab Emirates	345
Switzerland	308
United States	272
Belgium	136
Canada	90

Trade in Services	2015
Services exports, millions USD	177
Services imports, millions USD	716
Services trade balance, millions USD	-539
Main services exports, %	
Travel	49.4
Transport	22.2

Financial Flows	2015
ws, millions USD	276.36
Personal remittances, % of GDP	0.17

Demography	2015
Population, millions (or 543 in 000s)	0.543
Land area, km^2	156,000

ICT	2014
Share of ICT goods, % total exports	0.05
Share of ICT goods, % total imports	4.24

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html.

SURINAME

As a former Dutch colony, that became independent in 1975, the legal system of Suriname is closely based on Dutch law. Its Constitution dates from 1987.

1.1 E-transactions law

A draft law on electronic transactions has been drafted, Wet *Elektronische* Transacties, based on the UNICTRAL Model Laws, but not yet adopted.

1.2 Consumer protection

A draft law on consumer protection has been drafted, Conceptwet Consumentenbescherming.

1.3 Data protection and privacy

Privacy is expressly protected under Article 17 of the Constitution.

1.4 Cybercrime and cybersecurity

A law criminalizing stalking and harassment has been adopted (Act No. 70 of 2012), which provides for the imposition of restrictive communication measures on perpetrators, including a prohibition on making contact through computers or the Internet (Art. 1(4)(c)), for a period of up to 60 days. The Act also inserts a new offence of 'stalking' into the Criminal Code, which focuses on conduct that "deliberately infringes another's privacy" (Art. 345b).

The Telecommunications Act (No. 151 of 2004)('TA') contains a general prohibition on interception, except for national security purposes (Art. 32). All public service providers are obliged to ensure that their systems are capable of being intercepted (Art. 33).

1.5 Online content

No further information is available.

1.6 Domain names

Under the TA, the Suriname Telecommunications Authority has responsibility for the management of 'numbers' (§ 5), which are broadly and would seem to potentially include domain names.[77] However the ccTLD .sr is currently managed by Telesur.[78]

J. TRINIDAD AND TOBAGO

Economy	2015
GDP, current USD (state as millions - is $29.5 billion)	29,511
GDP per capita, current USD	21,698
Real GDP growth, y-on-y, %	-0.04

Merchandise Trade	2015
Merchandise exports, millions USD	11,100
Merchandise imports, millions USD	7,900
Merchandise trade balance, millions USD	3,200
Main marchandise exports, %	
Fuels	57
Manufactured goods	38
T exports, millions USD	
United States	5,071
Spain	677
Jamaica	581
United Kingdom	323
Barbados	291

Trade in Services	2010
Services exports, millions USD	874
Services imports, millions USD	389
Services trade balance, millions USD	485
Main services exports, %	
Travel	51.4
Transport	25.5

Financial Flows	2015
ws, millions USD	1,618.61
ws, millions USD	1,954.62

Demography	2015
Population, millions	1.360
Land area, km^2	5.130

ICT	2010
Share of ICT goods, % total exports	0.05
Share of ICT goods, % total imports	3.07

Source: UNCTADstat, 2016, http://unctadstat.unctad.org/EN/Index.html

TRINIDAD AND TOBAGO

In June 2015, the then Ministry of Science and Technology, which had responsibility for ICT, revised the 2005 policy document 'National Policy on Electronic Transactions', which was the basis for the adoption of the Electronic Transactions Act (No. 6 of 2011) ('ETA'). The objectives of the policy include the need to remove barriers to the use of electronic commerce, including those based on legal uncertainties; establish a regulatory structure for trusted third parties and service providers; enable cross-border recognition and enforcement; harmonize national laws with international best practice; respect freedom of contract; adopt rules r market-driven standards; facilitate e-government; ensure an appropriate allocation of liability for intermediary service providers; enhance consumer trust and maintain the integrity of the Internet. As far as possible, these objectives should be achieved through 'a "light touch" co-regulatory approach' (at 5),? as well as embodying the principles of media neutrality, technological neutrality and functional equivalence.

1.1 E-transactions law

Trinidad and Tobago's ETA is partially proclaimed (Parts I, II, III, IV and VII) with the following elements to be announced:

- Part V: Electronic Authentication Service Providers
- Part VI: Intermediaries and Telecommunications Service
- Providers
- Part VIII: Consumer Protection
- Part IX: Contravention and Enforcement

Part II of the ETA grants legal recognition to electronic transactions and is based both on the UNCITRAL Model Law (1996) and the 2005 Convention. Likewise, for Part III, which addresses contract formation. Part IV covers the validity of electronic signatures and is based on the 2001 Model Law. However, such recognition is somewhat undermined by the failure to implement Part V, since only electronic signatures are deemed to satisfy the requirements for reliability and integrity outlined in the Act (s. 31). However, this has not prevented regulations referring to the use of 'electronic signatures' as a valid means of authentication and authorization.[79]

E-government is encouraged under Part VII by a general facilitation provision recognizing electronic forms of retention or issuance, despite any legal provisions to the contrary. A public body is, however, able to specify the manner and format, control procedures and processes and any required attributes of such electronic alternatives (s. 53(2)).

1.2 Consumer protection

General consumer protection measures are contained in the Consumer Protection and Safety Act (No. 30 of 1985). This established the post of Director of Consumer Guidance, who resides within the Ministry of Trade and Industry.

Online vendors are required to provide certain minimum information to consumers under Part VIII of the ETA, including in respect of electronic authentication products. A failure to provide such information grants a consumer a right of rescission in respect of any contract entered into (s. 57). The sending of unsolicited electronic commercial communications is a criminal offence unless the recipient is granted a means of opting-out of future such communications.

1.3 Data protection and privacy

A right to privacy is provided for under the Constitution.[80]

The Data Protection Act (No. 13 of 2011) ('DPA') is also partially proclaimed. It provides for the establishment of the of the Information Commissioner under Part II, which is currently being pursued. In September 2015, following a comprehensive Government reorganization, the Ministry of Communications was assigned responsibility for data protection. In March 2016, the Communications Ministry was merged with the Ministry of Public Administration to create the Ministry of Public Administration and Communications.[81]

The DPA requires all persons processing 'personal information' to comply with the twelve General Privacy Principles (s. 6). The Act then contains different rules for 'public bodies' (Part III) and the private sector (Part IV). It is envisaged that the private sector will also be subject to codes of practice, which build on the General Privacy Principles, developed by industry sectors or professional bodies, which may either be voluntary or mandatory.[82]

Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II of the Act have been proclaimed in order to facilitate the establishment of the of the Information Commissioner, which has primary responsibility for monitoring the administration of the Act. The other parts of the Data Protection Act to be proclaimed address the protection of personal data by public bodies and

the private sector as well as the enforcement of the provisions of the Act against contravention.

When fully enacted, the DPA will also amend the Freedom of Information Act (No. 26 of 1999) ('FOIA'), to ensure alignment with the DPA (s. 101). The FOIA exempts documents whose disclosure would involve "the unreasonable disclosure of personal information of any individual (including a deceased individual)" (s. 30). 'Personal information' is broadly with a non-exclusive list of categories. The public authority has an obligation, where practicable, to give the subject prior e to be challenged.

1.4 Cybercrime and cybersecurity

The Computer Misuse Act (No. 86 of 2000) ('CMA') is based on a UK statute with the same name, with additional offences for conduct targeting the , integrity and availability of computer systems, as well as the programs and data they contain. The applicable sanctions are enhanced where the offence involves a 'protected computer', which are those involved in the security and defence of the state, and those involved in the provision of critical infrastructure, such as services, public utilities and communications (s. 9(2)). A court may also impose a compensation order on a convicted person.

Although primarily concerned with criminal conduct, the CMA also contains provisions granting the police certain powers to search, access and seize computers or copy any program or data in the course of an investigation (s. 16). The exercise of such powers must be authorized by a Magistrate, who can also direct an 'authorized person' to accompany the police such as a forensic expert. Persons associated with any computers being searched can be required to assist, including the provision of any information that can enable access to encrypted information. Failure to comply is an offence, with a maximum tariff of two years imprisonment.

The powers of law enforcement agencies to engage in network forensics are governed by the Interception of Communications Act (No. 11 of 2010).[83] The Act begins by criminalizing the interception of communications in the course of transmission, imposing a maximum penalty of seven years imprisonment. The offence supplements the offence of unauthorized interception of a computer service, at section 6 of the CMA. However, the vast majority of the Act concerns criminal procedure, the rights of law enforcement to intercept communications and demand access to communications data held by providers of 'telecommunication services'. Intercept requires a judicial warrant (s. 8) and service providers have a duty to assist (s. 13). Complementing the decryption power under the CMA, a judge may require key disclosure to enable access to a 'protected communication' (s. 15), although this excludes keys only used to generate electronic signatures.

In 2014 and 2015, attempts were made to strengthen the legal regime against cybercrime and improve cybersecurity, in two bills introduced into Parliament: The Cybercrime Bill and the Trinidad and Tobago Cyber Security Agency Bill 2015.[84] The former would have repealed and replaced the CMA, with a set of new offences and enforcement powers. The latter would have established a new agency for cybersecurity matters. Both bills lapsed in June 2015, primarily due to objections by the media about the implications of the Cybercrime Bill.[85] The Cybercrime Bill is currently on the Legislative Agenda while the Cyber Security Agency Bill has been withdrawn as it was determined that the Ministry of National Security would make internal arrangements to address cybersecurity matters. In this regard, it is to be noted that a Computer Security Incident Response Team (CSIRT) has been established within that Ministry.

1.5 Online content

Part VI of the ETA will provide 'intermediaries' and telecommunication service providers with protection from liability for content for which they 'merely provide a conduit'. Service providers would also not be required to pro-actively monitor any content that they process on behalf of others (s. 50(3)). As well as a general immunity from tortious or criminal liability, service providers would be granted a immunity from liability for infringements of copyright and related rights during the course of an 'audit' carried out under the Copyright Act (s. 50(4)). Service providers would also be required to comply with certain procedures where they obtain 'actual knowledge' that content may attract civil or criminal liability (s. 51). The Cybercrime Bill (see 2.10.4 above) is expected to introduce more comprehensive provisions to protect intermediaries from liability when engaged in a range of activities, including the provision of hosting services, hyperlinking and search engines.

1.6 Domain names

The ccTLD .tt is managed by the Trinidad and Tobago Network Information Centre.[86]

ANNEXES

Table 5. Detailed status of e-commerce law harmonization in the Caribbean as of December 2016

	Electronic Transactions Law	Consumer Protection	Data Protection and Privacy	Cybercrime and Cybersecurity	Online Content	Domain Names
Antigua and Barbuda	Electronic Transactions Act 2006 (ETA)	Consumer Protection and Safety Act 1988 (Cap. 97) Unfair Contract Terms Act 1987 (Cap. 451) (currently reviewed) Electronic Transactions Act 2006, Part IX, (ETA) Electronic Funds Transfer Crimes Act 2007 (Cap. 292)	Constitution Data Protection Act 2013 (DPA) Freedom of Information Act 2004 (FOIA) Electronic Transactions Act 2006 (ETA)	Electronic Crimes Act 2013 (ECA) Electronic Funds Transfer Crimes Act 2007 Prevention and Prohibition of Unauthorized Use and Services Act 1994 Computer Misuse Act 2006	Electronic Transactions Act 2006, Part VIII (ETA)	Draft Telecommunications Bill 2007
The Bahamas	Electronic Communications and Transactions Act 2006 (ECT)	Unfair Terms in Consumer Contracts Act 2006	Privacy of Personal Information Act 2003	Computer Misuse Act 2003, Sections 9, 1, 12 Criminal Procedure Code (Chap. 91)	Electronic Communications and Transactions Act 2006, Part III (ECT)	Electronic Communications and Transactions Act 2006 (ECT)
Barbados	Electronic Transactions Law in 2001 (ETA)	Consumer Protection Act 2002 (Cap. 326D)	Constitution of Barbados Electronic Transactions Law in 2001 (ETA) Draft eData Protection Bill	Computer Misuse Act 2005 (CMA) Telecommunications Act 2001 (Cap. 282B)	Electronic Transactions Law in 2001 (ETA)	Telecommunications Act 2001
Costa Rica	Firmas Digitales y Documentos Electrónicos, 2005 Public Procurement Act (No. 7494 of 1995)	Law on Promotion of Competition and Effective Consumer Defense (No. 7472 of 1994)	The Constitution Law of Protection of the Person in the Processing of His Personal Data	Penal Code, amendment in 2001 and 2012	None	Domain Deletion Policy
Cuba	eCommerce Decree (under review) Resolution 61/2002	None	Constitution 1976	Resolution on "Safety Regulations for Information Technology" The Penal Code (Act No. 62 of 1987, as amended by Act No. 97 of 1999)	None	Resolution 280/2015
El Salvador	Draft 2001, Ley de Comercio Electronico y Comunicaciones Civil and Commercial Code Banking Act 1999 Law on Electronic Annotations Securities Account 2002 Customs tion Act	Constitution Consumer Protection Act 2005 (Decree No. 776) Ley de Protección al Consumidor, Reformada 2013	Constitution, article 2 Decree No. 695, No. 141 Customs tion Act	Draft 2015, Ley Especial Contra Los Delitos Informaticos y Conexos Special Law against Acts of Terrorism (2006) Special Law to Sanction Customs Violations (2001)	None	Law on Trademarks and Other Distinctive Signs (Decree No. 868, 2006)

Table 5. Detailed status of e-commerce law harmonization in the Caribbean as of December 2016

	Electronic Transactions Law	Consumer Protection	Data Protection and Privacy	Cybercrime and Cybersecurity	Online Content	Domain Names
Jamaica	Electronic Transactions Act (Act 15 of 2006) (ETA)	Trade Act 1955 Consumer Protection Act (Act 9 of 2005) Electronic Transactions Act (Act 15 of 2006), Part IV (ETA) Telecommunications Act (Act 1 of 2000), Part VII (TA)	Constitution Electronic Transactions Act (Act 15 of 2006) (ETA) Trade Act 1955	Cybercrimes Act 2010 Interception of Communications Act (Act 5 of 2002)	Electronic Transactions Act (Act 15 of 2006) (ETA)	None
Saint Lucia	Electronic Transactions Act (No. 16 of 2011) (ETA)	Electronic Transactions Act, Part V (No. 16 of 2011) (ETA)	Constitution 2006 Data Protection Act (No. 11 of 2011)	Criminal Code (Act 9 of 2004) Computer Misuse Act (No 12 of 2011) (CMA) Electronic Crimes Bill (not yet in force)	Electronic Transactions Act (No. 16 of 2011) (ETA)	Telecommunica-tions Act (No. 27 of 2000)
Suriname	Draft, Wet Elektronische Transacties	Draft, Conceptwet Consumentenbes-cherming	Constitution, article 17	Act No. 70 of 2012 Telecommunica-tions Act (No. 151 of 2004) (TA)	None	Telecommunica-tions Act (No. 151 of 2004) (TA)
Trinidad and Tobago	Electronic Transactions Act (No. 6 of 2011) (ETA)	Consumer Protection and Safety Act (No. 30 of 1985)	Constitution Data Protection Act (No. 13 of 2011) (DPA)	Computer Misuse Act (No. 86 of 2000) (CMA) Cyber Crime Bill 2014 (not yet passed in parliament)	Electronic Transactions Act (No. 6 of 2011), Part VI (ETA)	None

Source: UNCTAD, 2016.

NOTES

1 LACNIC/CAF. "IPv6 Deployment for Social and Economic Development in Latin America and the Caribbean." 2015. http://docplayer.net/26500139-Ipv6-deployment-for-social-and-economic-development-in-latin-america-and-the-caribbean.html

2 UNCTAD. B2C E-commerce Index 2016. http://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d07_en.pdf.

3 https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

4 ol. XXVI, No. 73 dated 7th December, 2006.

5 http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf and http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf, respectively.

6 E.g. ISO/IEC 27037: 2012 'Information technology – Security techniques - Guidelines for collection, acquisition, and preservation of digital evidence'.

7 Articles 3(c) and 10 respectively.

8 The idea of a 'Data Pr oposed in a draft bill dating back to 2003.

9 http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf.

10 It was amended in 2003.

11 EU Directive 00/31/EC 'on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce); OJ L 178/1, 17.7.2000, at arts. 12-15.

12 http://telecom.gov.ag.

13 http://www.laws.gov.ag/bills/2007/Telecommunications_2007.pdf.

14 Section 6(j).

15 http://www.nic.ag.

16 http://www.nic.ag/policies.htm.

17 http://www.bahamas.gov.bs/wps/wcm/connect/mof_content/internet/all%20pdfs/resources/ecommerce%20policy%20statement.

18 http://www.bahamas.gov.bs/dataprotection.

19 Section 2: "a person who uses electronic means in providing goods and services".

20 The Electronic Transaction (Amendment) Act 2014, available in its Bill form at http://www.commerce.gov.bb/website/index.php/legislation.

21 Directive 99/93/EC 'on a Community framework for electronic signatures'; OJ L 13/12, 19.1.2000.

22 www.ftc.gov.bb.

23 https://www.icpen.org.

24 http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024631.pdf.

25 http://www.commerce.gov.bb/images/document_pdf/computer_misuse_act_2005-4.pdf.

26 https://www.itu.int/net/pr ess_releases/2013/CM09.aspx.

27 www.telecoms.gov.bb.

28 http://www.telecoms.gov.bb/website/Documents/Policies/PDF/Top%20Level%20Domain%20Name%20Policy.pdf.

29 Ley No. 8454, La Gaceta, No 197, 13 October 2005; available at http://www ley%208454.pdf (Spanish).

30 http://www

31 Regulation of the Law of Digital Signatures and Electronic Documents, Executive Decree No. 33018-MICIT of 20 March 2006, available at http://www etoNum33018.pdf.

32 Guideline No. 067-MICITT-H-MEIC, 25 April 2014.

33 Ley de Servicios de la Sociedad de la Información (Ley de Comercio Electrónico), Expediente Nº 19.012, La Gaceta No 117, 19 Junio 2014.

34 A/RES/39/248, 16 April 1985.

35 Executive Decree No. 37899-MEIC, 23 September 2013.

36 Law 8968, enacted on 5 September 2011, available at http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf (Spanish).

37 Published 5 March 2013, available at http://www.redipd.org/legislacion/common/legislacion/costa_rica/Decreto_37554JP20102012Re glamentolCostaRica.pdf (Spanish).

38 http://www.redipd.es/actividades/seminarios_2007/common/diirectivas_harmonizacion-sem_2007_en.pdf.

39 http://www.prodhab.go.cr.

40 https://www.unodc.org/res/cld/document/cri/1970/codigo_penal__html/Codigo_Penal.pdf.

41 https://www.nic.cr/es/.

42 Resolution No. 49/2001.

43 http://www.bc.gob.cu/Espanol/manual_regulaciones.asp.

44 Resolution No. 127/2007, available at http://www.mincom.gob.cu/?q=marcoregulatorio or *Gaceta* No. 057 Ordinaria de 30 de agosto de 2007.

45 http://www.cscuba.cu/es/node/221.

46 Agreement No. 6058 of the Executive Committee, 9 July 2007.

47 http://www.mincom.gob.cu/?q=marcoregulatorio.

48 http://www.nic.cu/.

49 http://www.bnamericas.com/en/news/technology/el-salvador -network2.

50 Dated 27 November 2008 and amended on 31 May 2010.

51

52

53 Anexo de la Resolución No. 224-2008 (COMIECO-XLIX).

54 Ley de Protección al Consumidor (Reformada 2013).

55 Decr nal No. 51.

56 Decr

57

58

59 http://enlaceacademico.ucr.ac.cr/node/2837.

60

61

62 As amended by Legislative Decree No. 913 (2006) and Decree No. 986 (2006).

63 https://www.icann.org/resources/pages/help/dndr/udrp-en.

64 http://www.svnet.org.sv.

65 http://unpan1.un.org/intradoc/groups/public/documents/caricad/unpan009914.pdf, at p. 12.

66 Drafted by the then Central Information Technology in the Ministry of Industry, Technology, Energy and Commerce.

67 http://www.tradeboard.gov.jm/tblweb/index.php?menuID=42.

68 http://www.consumeraffairsjamaica.gov.jm.

69 Directive 2011/83/EU, OJ L 304/64, 22.11.2011.

70 T lation (No. 17 of 2002).

71 The former is information about the subscriber, such as martial status, that is unrelated or incidental to the provision of the services; while the latter concerns the usage of the services made by the subscriber (ibid., at r. 3).

72 Ibid., at r. 12.

73 http://www.ntrc.lc.

74 http://www.nic.lc/index.html.

75 http://www.ectel.int/index.php.

76 Available at http://www.ntr onic%20Communication%20Bill%20-%20Revised%20draft%20 12_10_15-2.pdf.

77 Art. 1(q): "digits, letters or other symbols whether or not in combination that serve for access to or of consumers, connection points, providers of telecommunications infrastructure and providers of telecommunications services".

78 https://www.register.sr/index.php.

79 E.g. Exchequer and Audit (Electronic Funds Transfer) Regulations 2015, at r. 7.

80 Section 4(c).

81 Trinidad and Tobago Gazette (Extraordinary), Vol. 54, No. 97, September 2015.

82 Christo, E., 'Data protection in Trinidad and Tobago', p.202-209, *International Data Privacy Law*, vol.3, no. 3, 2013.

83 Amended by Act No. 14 of 2010.

84 See http://www.ttparliament.org/publications.php?mid=28.

85 Trinidad and Tobago Guardian, 'Debate stalled on Cybercrime bill', 21 May 2015.

86 https://www.nic.tt.

Layout and Printing at United Nations, Geneva – 1800624 **(E)** – February 2018 – 636 – **UNCTAD/DTL/STICT/2017/9**