International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

Jamaica's Electronic Transactions Act and Puerto Rico's E-Government Act: Paradigms for Fine-Tuning of E-Commerce Law in the Caribbean Region

Stephen Errol Blythe*
Department of Accounting, Finance and Economics
Tarleton State University
Fort Worth, Texas USA
Email: blythe@tarleton.edu
USA

ABSTRACT

The Caribbean Region has been experiencing an annual growth rate of 25% in B2C E-commerce. Nevertheless, some nations in the Region are lagging and need to reform their E-commerce laws to participate fully in the growth trend. They can look to the Jamaican and Puerto Rican statutes as models to emulate. Jamaica's Electronic Transactions Act (ETA) contains a third-generation E-signature law; all types of E-signatures are accepted, but a preference is given to the digital signature. The most distinguished sections of the ETA are the comprehensive provisions relating to the use of the electronic form to satisfy statutory requirements; legal liability of Certification Service Providers, subscribers, and relying on third parties; and the provisions relating to the effect of an error or omission occurring during an E-commerce communiqué. Despite these positive aspects, the ETA does need to be fine-tuned. Puerto Rico's E-Government Act (EGA) is exemplary because it: mandates the implementation of a comprehensive list of E-government services at the Government Portal; assigns one government agency the responsibility of implementation of E-government and gives it broad powers to achieve that goal; and establishes a long list of specific government services that government departments are required to provide citizens. This article makes recommendations for amendment of the ETA and presents the amended Jamaican ETA and the Puerto Rican EGA as paradigms for other Caribbean nations to follow.

Keywords: Caribbean, law, E-commerce, E-signature, E-contract

1. Objectives of the Article

The objectives of this article are to (1) consider the growth rate of E-commerce in the Caribbean Region; (2) explain the roles of electronic signatures, cryptology, public key infrastructure, and certification authorities; (3) describe the three generations of electronic signature law; (4) provide an overview of E-commerce laws in the Caribbean Region; (5) analyze Jamaica's Electronic Transactions Act (ETA) in some detail and make recommendations for its improvement; and (6) recommend the amended Jamaican ETA and the Puerto Rican Electronic Government Act as paradigms for other Caribbean nations to emulate.

2. Background: Recent Growth in Caribbean E-Commerce

The Caribbean Region has a population of approximately 43 million and its internet penetration is over 50%.[1] E-commerce B2C sales in the Caribbean Region are valued at the U.S. $5 billion annually and is growing at the impressive rate of 25% per year.[2] During Covid-19, online buying has increased because consumers want to avoid face-to-face contact when making their purchases. Greater online buying is expected to continue after the pandemic because customers have become comfortable with the process and appreciate its convenience.[3] During Covid-19, credit cards have become the most popular E-commerce payment method; customers found it more difficult to make cash payments due to the temporary shutdown of online payment platforms such as MoneyGram or Western Union.[4]

Despite those impressive statistics, E-commerce is still in its infancy in the Caribbean Region and is far from being a mature channel of distribution. One of the potential roadblocks to the continued growth of Caribbean E-commerce is the need for the implementation of effective E-commerce laws.[5] Most of the Caribbean nations have enacted E-commerce laws and an overview of them will be included in this article but many of those laws are flawed and need to be improved.

3. Electronic Signatures

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[6] With the onset of the electronic age, the electronic signature made its appearance. It has been defined as "data in electronic form which are attached to or logically associated with other

[1] Franz Weathers, "The Caribbean's First US$ 1 Billion Startup," Medium.com, January 19, 2019; https://medium.com/gobeyond-ai/the-caribbeans-first-us-1-billion-startup-45863b6a00c5.
[2] "E-Commerce in Jamaica Goes Hyper-Local Finally?," Silicon Caribe, April 9, 2020; https://www.siliconcaribe.com/2020/04/09/ecommerce-in-jamaica-goes-hyper-local-finally/ .
[3] Vanita Maharaj, "4 Steps for Small Business Owners in the Caribbean to Utilize Online Shopping," Alternative Concepts, June 3, 2020; https://www.acmarketingcaribbean.com/post/4-steps-for-small-business-owners-in-the-caribbean-to-utilize-online-shopping.
[4] Claire Shefchik, "Caribbean E-Commerce Gets a Boost from Covid," The BVI Beacon, May 21, 2020; https://www.bvibeacon.com/caribbean-e-commerce-gets-a-boost-from-covid/.
[5] Ed Kennedy, "The State of E-Commerce in the Caribbean," St. Lucia Star, February 18, 2018; https://stluciastar.com/state-e-commerce-caribbean/.
[6] See, e.g., United States, *Uniform Commercial Code* Sect. 2-201, 2-209 (1998).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

electronic data and which serve as a method of authentication."[7] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[8]

3.1. *E-Contracts: Four Levels of Security*

When entering into an E-contract, four degrees of security are possible.

1. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[9]

2. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased.[10]

3. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief. Examples include a voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, digital reproduction of a fingerprint,[11] or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison with a person purporting to have the same identity. For example, if a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter.[12]

Biometrics, despite its potential utility as a form of electronic signature, has at least two drawbacks in comparison with the digital signature: (1) The attachment of a person's biological traits to a document does not ensure that the document has not been altered, i.e., it "does not freeze the contents of the document;"[13] and (2) The recipient of the document must have a database of biological traits of all signatories dealt with to verify that a particular person sent the document.[14] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[15] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[16]

4. The digital signature is considered the fourth level because it is more complex than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document.[17] It is "the sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key." A digital signature has two major advantages over other forms of electronic signatures: (1) it verifies authenticity that the communication came from a designated sender; and (2) it verifies the integrity of the content of the message, giving the recipient assurance that the message was not altered.[18]

3.2. *Digital Signature Technology: Public Key Infrastructure*

The technology used with digital signatures is known as Public Key Infrastructure (PKI).[19] PKI consists of four steps:

1. The first step in utilizing this technology is to create a public-private key pair; the private key will be kept in confidence by the sender, but the public key will be available online.

2. The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it. A "hash value" is created by applying a "hash function" a standard mathematical function to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Whereupon, the hash function is encrypted, or scrambled, by the signatory using his private key. The encrypted hash function is the "digital signature" for the document.[20]

3. The third step is to attach the digital signature to the message and to send both to the recipient.

4. The fourth step is for the recipient to decrypt the digital signature by using the sender's public key. If decryption is possible the recipient knows the message is authentic, i.e., that it came from the purported sender. Finally,
the recipient will create a second message digest of the communication and compare it to the decrypted message

[7] European Union, *Directive1999/93/EC of the European Parliament and of the Council of13 December 1999 on a Community Framework For Electronic Signatures*, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12.
[8] David K.Y. Tang, "Electronic Commerce: American and International Proposals for Legal Structures," *Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries*, p. 333 (Christopher McCrudden ed., 1999).
[9] Jonathan E. Stern, Note, "Federal Legislation: The Electronic Signatures in Global and National Commerce Act," 16 *Berkeley Tech. L.J.* 391, 395 (2001).
[10] Id.
[11] In the highly successful Hong Kong Identity Card, the two thumb prints are used as a biometric identifier. See, Rina C.Y. Chung, "Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America," 4 *Asian-Pacific L. & Pol'y J.* 442 (2003).
[12] Id.
[13] K.H. Pun, Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan, "Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?," 32 *Hong Kong L.J.* 241, 256 (2002).
[14] Id. at 257.
[15] Id. However, one of the experts in computer law and technology—Benjamin Wright—is a notable exception. Wright contends that biometrics is a more preferable authentication method in the case of the general public, although he concedes that digital signatures using PKI are preferable for complex financial deals carried out by sophisticated persons. In PKI, control of the person's "private key" becomes all-important. The person must protect the private key; all of the "eggs" are placed in that one basket, and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public would be sharing the risk with other parties involved in the transaction, and the need to protect the "private key" is not so compelling. See, Benjamin Wright, "Symposium: Cyber Rights, Protection, and Markets: Article, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures,'" 32 *West L.A. L. Rev.* 215, 225-26 (2001).
[16] Note 11 supra.
[17] The Hong Kong E-commerce law typically defines a digital signature as follows: "an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine: (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was generated." China, Hong Kong Special Autonomous Region, *Electronic Transactions Ordinance*, Ord. No. 1 of 2000, s 2.
[18] Christopher T. Poggi, "Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation," 41 *Va. J. Int'l L.* 224, 250-51 (2000).
[19] Susanna Frederick Fischer, "California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation," Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, 7 *B.U. J. Sci. & Tech. L.* 229, 233 (2001).
[20] Note 18 supra at 249.

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

digest. If they match, the recipient knows the message has not been altered.[21]

3.3. Advantages of the Digital Signature

Unlike biometric and other forms of electronic signatures, the digital signature will "freeze" the contents of the document at the time of its creation. Any alterations to the document's contents will result in a different hash value. Furthermore, the encryption of the hash value with the signatory's private key "links uniquely the digital signature to the signatory, i.e., the owner of the private key."[22] Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific."[23]

The digital signature is the only form of electronic signature which satisfies all three of the UNCITRAL evaluation factors, i.e., that an electronic signature should:

(1) authorize; (2) approve, and (3) protect against fraud.[24] Authorization is achieved because the digital signature will accompany the document, which allows for confirmation of the identity of the signatory. Approval is attained via computation of the hash value of the electronic document, which freezes the contents of the document at the time of its creation, and allows for detection of any subsequent alterations. Finally, there is protection against fraud because it is extremely unlikely virtually impossible for anyone to determine a signatory's private key with only the public key as a starting point.[25]

3.4. *Disadvantages of the Digital Signature*

The digital signature has at least two drawbacks. Firstly, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common to most other forms of electronic signatures. The password or the PIN face similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized.[26]

The other disadvantage of the digital signature pertains to the digital certificate, which must be issued by a Certification Authority ("CA"). Obtaining the certificate and having to interact with the CA is somewhat inconvenient and costly for the user, but over time this disadvantage should be alleviated as digital signatures become more popular, easier to use, and cheaper.[27] Because the CA plays such a vital role in the viability of the digital signature, the user needs to understand exactly what the CA does.

3.5. The Critical Role of the Certification Authority

For PKI to realize its potential, the user must be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If Smith and Jones are attempting to consummate an online transaction, Smith needs an independent confirmation that Jones' message is actually from Jones before Smith can have faith that Jones' public key belongs to Jones. It is possible that an imposter could have sent Jones his public key, contending that it belongs to Smith. Accordingly, a reliable third party the Certification Authority (CA)[28] must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[29]

The most important job of the CA is to issue certificates that confirm basic facts about the subscriber, the subject of the digital certificate. Of course, the certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties. Typical information contained in a certificate includes the following: the name and address of the CA that issued the certificate; the name, address, and other attributes of the subscriber; the subscriber's public key; and the digital signature of the CA.[30] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[31]

In making an application to a CA for a certificate, the prospective subscriber must provide some sort of photo I.D., e.g., a passport or a driver's license. If the application is approved and the certificate is issued, the CA will issue a private key to its new subscriber which corresponds to the public key. This is done, however, without disclosing the specifics of the private key.[32] The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered by the CA. Ordinarily, however, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued.[33]

To indicate the authenticity of the digital certificate, the CA will sign it with her digital signature. Ordinarily, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties who need communication with the subscriber. Additionally, the online repository contains information about digital certificates which have been revoked or suspended by the CA due to lost or expired private keys. This is an important positive aspect of PKI technology: the general public has access to the status of digital signatures, and relying on third parties are kept informed, allowing them

[21] Jochen Zaremba, "International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers," 18 *Conn. J. Int'l L.* 479, 512 (2003).
[22] Note 18 supra at 250.
[23] Id.
[24] Note 18 supra at 243.
[25] Note 18 supra at 252.
[26] Note 18 supra at 253.
[27] Id.
[28] Certification Authority ("CA") seems to be the most commonly used designation in the world, but several other names are used. The European Union uses the term "Certification Service Provider," and this term has been adopted by Jamaica and several other Caribbean nations.
[29] Tara C. Hogan, Notes and Comments—Technology, "Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?," 4 *N.C. Banking Inst.* 417, 424-25 (2000).
[30] A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 *Or. L. Rev.* 49, 58 (1996).
[31] Note 29 supra at 425-426.
[32] Thomas J. Smedinghoff, "Electronic Contracts: An Overview of Law and Legislation," 564 PLI/P at 149 (1999).
[33] Id. at 150.

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

to judge whether they should place reliance on communications signed with a certain private key.[34]

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber. Nations around the world, and the state laws of the United States, have arrived at different conclusions regarding this apportionment. The problem is compounded if each CA is required to modify its practices every time it issues a certificate about a transaction affecting another jurisdiction that happens to have dissimilar digital signature laws.[35]

A digital certificate is only as reputable as the CA who issued it. If the CA is unreliable and untrustworthy, the digital certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate.[36]

4. Three Generations of Electronic Signature Law

4.1. The First Wave: Technological Exclusivity

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[37] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[38] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature include Bangladesh, India[39], Malaysia, Nepal[40], and Russia.[41]

Unfortunately, these jurisdictions' decision to allow the utilization of only one form of technology is burdensome and overly restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's disadvantages: more expense, lesser convenience, more complication, and less adaptability to technologies used in other nations, or even by other persons within the same country.[42]

4.2. The Second Wave: Technological Neutrality

Jurisdictions in the Second Wave overcompensated. They did the complete reversal of the First Wave and did not include any technological restrictions whatsoever in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the others. In other words, they are "technologically neutral." Permissive jurisdictions provide legal recognition of many types of electronic signatures and do not grant a monopoly to any one of them. Examples of permissive jurisdictions include the majority of states in the United States,[43] the United Kingdom,[44] Australia, and New Zealand.[45]

The disadvantage of the permissive perspective is that it does not take into account that some types of electronic signatures *are* better than others. A PIN and a person's name typed at the end of an E-mail message are both forms of electronic signatures, but neither can even approach the degree of security that is provided by the digital signature.

4.3. The Third Wave: A Hybrid

Singapore was in the vanguard of the Third Wave. In 1998, this country adopted a compromise, middle-of-the-road position for the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce.[46] In terms of the relative degree of technological neutrality, Singapore adopted a "hybrid" model a preference for the digital signature in terms of a greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures. Singapore did not want to become "hamstrung" by tying itself to one form of technology. The Singapore legislators realized that technology is continually evolving and that it would be unwise to require one form of technology to the exclusion of others. The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[47]

Many nations have joined the Third Wave. They recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures. This preference is exhibited in several ways: (1) utilization of a digital signature using a PKI system is explicitly required for authentication of an electronic record; (2) utilization of a digital signature with PKI seems to be necessary for an electronic record to comply with any statutory requirement that a record is in paper form; and (3) for a signature in the electronic form to comply with a

[34] Note 29 supra at 426-27.
[35] Andrew B. Berman, Note, "International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 *Syracuse J. Int'l L. & Com.* 125, 143-44 (2001).
[36] David Hallerman, "Will Banks Become E-commerce Authorities?," 12 *Bank Tech. News,* June 1, 1999.
[37] *Utah Code Annotated* 46-3-101 *et seq.* (1999).
[38] Id.
[39] Stephen E. Blythe, "A Critique of India's Information Technology Act and Recommendations for Improvement," 34 Syracuse J. Int'l L. & Com. 1 (2006).
[40] Stephen E. Blythe, "On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law," 8:1 J. High Tech. L. (2008).
[41] Note 23 supra at 234-37.
[42] Sarah E. Roland, Note, "The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?" 35 SUFFOLK U. L. REV. 625, 638-45 (2001).
[43] For concise coverage of American and British law, see Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security," 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005).
[44] Id.
[45] Note 18 supra at 234-37.
[46] [10] United Nations Commission on International Trade Law ("UNCITRAL"), *Model Law on Electronic Commerce with Guide to Enactment* (MLEC), G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996).
[47] Republic of Singapore, *Electronic Transactions Act* (Cap. 88), 10 July 1998; Although granting legal recognition to most types of electronic signatures, the Singapore statute implicitly makes a strong suggestion to users—in two ways—that they should use the digital signature because it is more reliable and more secure than the other types of electronic signatures: (1) digital signatures are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carry a legal presumption of reliability and security—these presumptions are not given to other forms of electronic signatures; and (2) although all forms of electronic signatures are allowed to be used in Singapore, its electronic signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the of authenticity and integrity of electronic messages affixed to electronic signatures. Id. *See* Stephen E. Blythe, "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33 Ohio No. U. L. Rev. 525-562 (2006).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

statutory requirement that a pen-and-paper signature is affixed, it must be a digital signature created with PKI. Nevertheless, the Third Wave jurisdictions do not appear to be as technologically restrictive as those in the First Wave. They do not compel the E-commerce participant to use only the digital signature, *instead of* other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

The moderate position adopted by Singapore has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European Union[48] Armenia,[49] Azerbaijan[50] Bulgaria,[51] China[52] Colombia,[53] Croatia,[54] Dubai,[55] Finland,[56] Hong Kong,[57] Hungary[58] Iran,[59] Japan,[60] Lithuania,[61] Pakistan,[62] Peru,[63] Slovenia,[64] South Korea,[65] Taiwan,[66] Tunisia,[67] the United Arab Emirates,[68] Vanuatu,[69] and in the proposed statutes of Uganda.[70]

5. E-Commerce Law in the Caribbean Region: An Overview

5.1. *Anguilla*

Anguilla enacted its Electronic Transactions Act (ETA) in 2006.[71] The ETA: recognizes the legal validity of E-signatures and E-documents and their acceptability for purposes of satisfying a legal writing requirement, retention requirement, originality requirement, delivery requirement, and inspection requirement; states that E-signatures and E-documents are admissible in a court of law; contains E-contract rules relating to attribution, the effect of change or error, acknowledgment of receipt, and time and place of dispatch and receipt of the message; contains a third-generation E-signature law; recognizes legal validity of foreign certificates and foreign E-signatures; states that an E-signature will comply with notarization and acknowledgment requirements; contains rules relating to the liability of E-commerce sellers and internet service providers; provides for licensing and regulation of Information Security Service Providers (issuers of certificates), and contains a list of cybercrimes.[72]

5.2. *Aruba*

Aruba does not have an E-commerce law.

5.3. Antigua and Barbuda

The Electronic Transactions Act ("ETA"), enacted in 2006 and revised in 2013, contains a third-generation E-signature law.[73] Certification Authorities are referred to as Information Security Services, the only jurisdiction using this designation. Distinctive sections of the ETA include liability of intermediaries and internet service providers; E-contract rules pertinent to errors and omissions; and use of electronic form to comply with statutory requirements. The other E-commerce rules are commonplace. The weakest sections of the statute are those pertinent to suspension/revocation of certificates, and computer crimes, and related punishments.[74]

5.4. the Bahamas

The Electronic Communications Transactions Act ("ECTA"), enacted in 2003, recognizes the legal validity of the electronic form as evidence in court and in contracting.[75] E-contract rules are provided about: attribution; acknowledgment of receipt; and time/place of transmission/reception. However, the E-commerce buyer is not protected, except for the fact that consumer notice requirements already established in other statutes may be given in the electronic form. The electronic form may be used to fulfill statutory requirements pertinent to writing; signature; notarization; delivery; originality; and retention. The statute contains a second-generation E-signature law; all types of E-signatures are recognized. An E-signature is defined, but there is no definition of a digital signature and no mention is made of Certification Authorities; these are deficiencies. Furthermore, the list of computer crimes and punishments is too general and needs to be expanded.[76]

[48] For concise coverage of European Union law, *see* Stephen E. Blythe, "E-Signature Law and E-Commerce Law of the European Union and its Member States," *Ukrainian J. Bus. L.*, pp. 22-26, May, 2008.
[49] Stephen E. Blythe, "Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security," *Armenian L. Rev.*, May, 2008.
[50] Stephen E. Blythe, "Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region," 1:1 *Columbia J. East European L.* 44-75 (2007).
[51] Stephen E. Blythe, "Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions," 17:2 *Transnat'l L. & Contemp. Problems* 361 (2008).
[52] Stephen E. Blythe, "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce," 7 *Chicago-Kent J. Intellectual Prop.* 1 (2007).
[53] Stephen E. Blythe, "Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act," a book chapter in *Internet Policies and Issues*, Frank Columbus, Ed., Nova Science Publishers, Inc., New York NY USA, 2009.
[54] Stephen E. Blythe, "Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security," 26: 1 *European J. L. & Econ*. 75-103 (August, 2008).
[55] Stephen E. Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. *See* Stephen E. Blythe, "Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's 'Most Wired' City," 7 *N.C. J. L. & Tech*. 1 (2005).*Econ. & Admin. Sciences* 103 (2007).
[56] Stephen E. Blythe, "Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services," 31:2 *Hamline L. Rev.* 445-469 (2008).
[57] Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. *See* Stephen E. Blythe, "Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's 'Most Wired' City," 7 *N.C. J. L. & Tech*. 1 (2005).
[58] Stephen E. Blythe, "Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions," 16:1 *Info. & Comm. Tech. L.* 47-71 (2007).
[59] Stephen E. Blythe, "Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World," 18 *Sri Lanka J. Int'l L.* (2006).
[60] Stephen E. Blythe, "Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access," 10 *J. Internet L.* 20 (2006).
[61] Stephen E. Blythe, "Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions," 8 *Barry L. Rev.* 23 (2007).
[62] Stephen E. Blythe, "Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce," 2:2 *J. Islamic State Practices in Int'l L.* 5 (2006).
[63] Note 59 supra.
[64] Stephen E. Blythe, "Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions," 6: 4 *I.C.F.A.I. J. Cyber L.* 8-33 (2007).
[65] Stephen E. Blythe, "The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation," 28:3 *Houston J. Int'l L.* 573-661 (2006).
[66] Stephen E. Blythe, "Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security," *Proceedings of the Sixth Annual Hawaii Int'l Conference on Business* (2006).
[67] Stephen E. Blythe, "Computer Law of Tunisia: Promoting Secure E-Commerce Transactions with Electronic Signatures," 20 *Arab L. Q.* 317-344 (2006).
[68] Stephen E. Blythe, "The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate," *Proceedings of the Annual International Conference on Global Business*, Dubai, United Arab Emirates (2009).
[69] Stephen E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga," 10:1 *J. So. Pacific L.* (2006).
[70] Stephen E. Blythe, "The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control," *Proceedings of the Tenth Annual Conference of the International Academy of African Business and Development*, Kampala, Uganda (2009).
[71] Anguilla, Electronic Transactions Act, Chapter E38, 2006; http://www.gov.ai/laws/E038-Electronic%20Transactions%20Act/ .
[72] Id.
[73] Antigua and Barbuda, ELECTRONIC TRANSACTIONS ACT ("ETA"), 2013; http://laws.gov.ag/wp-ontent/uploads/2019/04/Electronic-Transactions-Act-2013.pdf.
[74] Id.
[75] Commonwealth of the Bahamas, ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT ("ECTA"), 2003; http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004ElectronicCommunicationsandTransactionsAct_1.pdf.
[76] Id.

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

5.5. Barbados

The Electronic Transactions Act ("ETA") was enacted in 2003.[77] The ETA's most remarkable aspects are allowance of the electronic form to comply with a statutory requirement for delivery of information; rules regarding when a receiver may assume a purported sender has transmitted an E-message; creation of a duty to maintain the confidentiality of information even if it was generated outside of Barbados; and a default punishment for computer crimes. The statute is weakened by: four exclusions from coverage; its non-mandatory E-government provisions; non-mandatory licensing of a CA; no list of specific acts of a CA which would justify revocation of its license, and no provision for mere suspension of a license; and its failure to list specific computer crimes.[78]

5.6. *Bermuda*

Bermuda enacted its Electronic Transactions Act (ETA) in 1999.[79] The ETA: requires wills and conveyance of real property to be in a paper document; contains a third-generation E-signature law; allows records to be retained in electronic form; provides the equal evidentiary weight of electronic evidence in a court of law; recognizes the legal validity of E-contracts; contains commonplace rules regarding attribution of the sender of a communique and the time and place of dispatch of a communique; regulates the licensing of Certification Service Providers (CSP) and their potential liability, and it contains encryption rules. The ETA established an Electronic Commerce Advisory Board to advise the Prime Minister on matters relating to this statute. At the end of the ETA, there is a list of other statutes that are amended by the ETA. There is no list of cybercrimes, but it does state that if a corporation violates the ETA, then all directors and officers of that corporation will be legally liable. The ETA does not provide for: E-Government to be accessed directly by citizens; IT Courts; consumer protections for those engaged in E-commerce; reciprocal recognition of foreign CSPs; or E-wills.[80]

5.7. *the British Virgin Islands*

The British Virgin Islands enacted its original Electronic Transactions Act (ETA) in 2001 and it was revised in 2019.[81] The revised ETA: excludes use of the electronic form for wills, trusts, conveyance of real property, immigration matters, and deeds; provides for legal recognition of E-documents and states that E-documents can be used to comply with legal requirements relating to writing, provision of copies, provision of information, provision of access to information, delivery of information, delivery of an original, or retention of records; provides E-contract rules for attribution, time and place of dispatch and receipt and use of automated message systems; contains a third-generation E-signature law and characteristics of a secure E-signature; contains regulations for Electronic Commerce Service Providers; requires E-commerce sellers to communicate honest information to buyers and provides for a maximum punishment of a fine of $200,000 and five years' imprisonment. The ETA does not include I.T. Courts, E-government, or a comprehensive list of cybercrimes.[82]

5.8. *Cayman Islands*

The Electronic Transactions Law ("ETL") was enacted in 2000 and revised in 2003.[83] The most exemplary provisions of the ETL are: electronic compliance with a statutory requirement for a notarized handwritten signature; electronic compliance with a statutory requirement for a document or information to be presented for public inspection; the reliability requirements of an E-signature; the E-contract rule concerning the effect of a change or an error; the requirement for a CA to disclose a subscriber's personal information to law enforcement authorities if requested to do so; the four categories of personal information not required to be kept confidential by a CA; the internet service provider regulations; and creation of the E-Business Advisory Board. The ETL is weakened by its three exclusions from coverage and its non-mandatory E-government provisions.[84]

5.9. Cuba

Cuba does not have an E-commerce law.

5.10. *Dominica*

The Commonwealth of Dominica enacted its Electronic Transactions Act ("ETA") in 2005.[85] The ETA contains a second-generation E-signature law. An E-signature is defined, but no mention is made of a digital signature or a Certification Authority. E-documents and E-signatures are legally valid (regardless of whether made domestically or in a foreign country) and they may be used to comply with statutory requirements about writing; prescribed form; signature; originality; and retention. E-contracts are just as valid as paper contracts if all parties agree to their use. Rules regarding attribution and time/place of sending/receiving are included. E-government is encouraged, though neither the government nor citizens are compelled to use the electronic form.[86]

5.11. Dominican Republic

The Dominican Republic enacted the E-Commerce Law (hereinafter "ECL") in 2002.[87] The ECL contains a first-generation E-signature law; the only type of electronic signature recognized is the digital signature. A compulsory

[77] Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B (ETA), 8 March 2001; http://admin.theiguides.org/Media/Documents/Electronic%20Transactions%20Act.pdf.
[78] Id.
[79] Bermuda, ELECTRONIC TRANSACTIONS ACT (ETA), 1999; http://www.bermudalaws.bm/laws/Consolidated%20Laws/Electronic%20Transactions%20Act%201999.pdf
[80] Id.
[81] British Virgin Islands, Electronic Transactions Act, 2019; https://bvi.gov.vg/sites/default/files/electronic_transactions_act_2019_1.pdf.
[82] Id.
[83] ayman Islands, ELECTRONIC TRANSACTIONS LAW, 200n3 (ETL); https://laws-in-force.judicial.ky/WebSearchFileView.aspx?fileView=E%5CElectronic%20Transactions%20Law%20(2003%20Revision).pdf.
[84] Id.
[85] Commonwealth of Dominica, ELECTRONIC TRANSACTIONS ACT ("ETA"), 2013; http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf . Note: the Commonwealth of Dominica should not be confused with the Dominican Republic, to be covered next.
[86] Commonwealth of Dominica, ELECTRONIC TRANSACTIONS ACT ("ETA"), 2013; http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf . Note: the Commonwealth of Dominica should not be confused with the Dominican Republic, to be covered next.
[87] Dominican Republic, LAW NO. 126-02 CONCERNING ELECTRONIC COMMERCE, DOCUMENTS, AND DIGITAL SIGNATURES ("ECL"), 2002; https://indotel.gob.do/media/5129/ley-no-126-02-ingles.pdf .

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

licensing system has been established for Certification Authorities; they are referred to as "Certifying Entities." Detailed regulations (promulgated by the DTI) are contained in the E-Commerce Regulations. Notable aspects of the ECL include: statutory retention requirements may be met with either an E-document or E-message, and four requirements are necessary for compliance; notice requirements for CE's and subscribers in termination of their contract; blanket liability of CE's; and mandatory E-government.[88]

5.12. *Grenada*

Grenada enacts its Electronic Transactions Act (ETA) in 2013.[89] The ETA: provides that real property conveyance, wills, trusts, and immigration documents must be in paper form; allows E-documents to comply with records retention requirements; allows E-documents to comply with the requirement to convey information; recognizes the admissibility of E-documents in a court of law; recognizes the legal validity of E-contracts and includes commonplace rules relating to time of dispatch and receipt of an offer and acceptance; contains a third-generation E-signature law; refers to Certification Service Providers as "Information Security Procedure" Providers and provides that the Prime Minister shall issue regulatory rules for them; provides for a basic level of E-Government by providing that governmental departments may establish E-government services for citizens; provides that the Prime Minister may establish a Code of Conduct for E-commerce sellers and buyers; creates rudimentary consumer protections by requiring E-commerce sellers to disseminate honest information regarding their goods and services; and states that the maximum punishment for violation of the ETA will be a fine of $500,000 and/or imprisonment for six years. The following items are missing: specific regulations for the Information Security Procedure Providers; an E-Government portal, I.T. Courts, extensive consumer protections; and a list of specific cybercrimes.[90]

5.13. *Haiti*

E-commerce is a slow-growing sector in Haiti, constrained by limited internet infrastructure and regulation. The Haitian Parliament recently enacted the Decree on Electronic Transactions making E-signature and E-contracts legally binding, but no further action to improve laws governing credit banking practices has been undertaken.[91]

5.14. *Montserrat*

Montserrat enacted its original Electronic Transactions Act (ETA) in 2009 and it was revised in 2011 and 2013.[92] The ETA: recognizes that E-documents have legal validity, except for wills; allows E-documents to comply with legal requirements for a writing, delivery, inspection, originality, or retention; provides that E-documents are admissible evidence in a court of law; contains E-contract rules relating to attribution, effect of change or error, acknowledgement of receipt, and time and place of dispatch and receipt; contains a third-generation E-signature law; recognizes the legal validity of foreign certificates; provides that a secure E-signature may be used to comply with Notarization or Acknowledgement requirements; provides for the licensing and regulation of Information Security Service Providers; provides for regulation and potential liability of internet service providers and E-commerce sellers; allows the Governor to issue regulations for protection of electronic data; allows the Governor to establish a Code of Practice relating to requirements and responsibilities of E-commerce sellers and to establish consumer protections for E-commerce buyers. The ETA is commendable in that wills is the only type of document mandated to be in paper form. However, the ETA fails to include I.T. Courts and a list of cybercrimes and punishments; furthermore, the statute should have included a comprehensive list of consumer protections instead of asking the Governor to promulgate those regulations.[93]

5.15. Netherlands Antilles

Netherlands Antilles enacted its Electronic Contracts Act (ECA) in 2000.[94] The ECA: requires E-sellers not to continue to send uninvited advertisements after they have been objected to and creates other rules for E-sellers requiring honesty; contains rules for the consummation of an E-contract and how to deal with errors during negotiations; contains a first-generation E-signature law; provides that E-signatures secured by a certificate shall be admissible evidence in a court of law; established rules for internet service providers; contains rules about the confidentiality of information and right of privacy; recognizes the legal validity of cryptographic techniques; created a Board for out-of-court settlement of disputes under this Act; created the office of the regulator entrusted with the responsibility of administration of this Act and enumerated the duties of that office; and provided for penalties for anyone convicted of violations of this Act.[95]

5.16. *Puerto Rico*

Puerto Rico has enacted the Uniform Electronic Transactions Act ("UETA") in its entirety.[96] The overriding majority of U.S. jurisdictions 45 states, the District of Columbia, and the Territories of Puerto Rico and the Virgin Islands have done so. The UETA contains a second-generation E-signature law. Accordingly, most types of E-signatures are legally recognized, provided they possess the four common trustworthiness attributes: uniqueness to the user; capability of verification; under the sole control of the user; and linked to the data in such a manner that if the data is changed, the signature is invalidated. If all four criteria are met, the E-

[88] Id.
[89] Grenada, Electronic Transaction Act, 2013; https://gov.gd/sites/hop/files/Acts-SROs/2013/Act%20No.%2021%20of%202013%20Electronic%20Transactions.pdf
[90] Id.
[91] U.S. Department of Commerce, Haiti—Country Commercial Guide, 2020; https://www.trade.gov/country-commercial-guides/haiti-ecommerce .
[92] Montserrat, Electronic Transactions Act, Chapter 11.32, 2013; http://agc.gov.ms/wp-content/uploads/Electronic-Transactions-Act.pdf .
[93] Id.
[94] Netherlands Antilles, Electronic Contracts Act, 2000; https://www.uaipit.com/uploads/legislacion/files/0000000241_State%20Ordinance%20Agreements%20via%20Electronic%20Channels-Eng.pdf .
[95] Id.
[96] 10 L.P.R.A. s 4081 et seq. (2007).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

signature will be enforceable.[97] Puerto Rico has also enacted the Electronic Government Act ("EGA").[98] The EGA is exemplary because it: mandates the implementation of a comprehensive list of E-government services at the Government Portal; assigns the OMB the responsibility of implementation of E-government and gives it broad powers to achieve that goal and establishes a long list of specific government services that the agencies are required to provide citizens. The government may decline to offer online services only if doing so would be unreasonable, impracticable, or illegal. The most important aspect of the EGA is its mandatory nature, unusual because most E-government statutes do not require agencies to provide online services, but merely encourage them to do so.[99]

5.17. *Saint Christopher and Nevis*

Saint Christopher and Nevis enacted its Electronic Transactions Act (ETA) in 2011 and it was revised in 2017.[100] The ETA: requires powers of attorney, wills, trusts, notarized documents, conveyance of real estate, and authentication of a document when the original does not exist, to be in paper form; provides for legal recognition of an E-document as a substitute for an original paper document; states that E-documents can be used to comply with records retention requirements; provides for the admissibility of E-documents in a court of law; establishes basic E-governments by allowing citizens to file E-documents and by allowing the government to issue E-documents to citizens; created E-contract rules relating to attribution, acknowledgment of receipt, and time and place of dispatch and receipt of the communique; contains a third-generation E-signature law; provided for regulation of Certification Service Providers; contains rules for E-commerce buyers and sellers, and established the E-Commerce Advisory Board to advise the Prime Minister on E-commerce matters. Conspicuous by their absence are specific consumer protections; I.T. Courts; and a list of cybercrimes and punishments.[101]

5.18. *Saint Lucia*

St. Lucia drafted an Electronic Transactions Bill in 2007 but it has not been enacted.[102]

5.19. *Saint Vincent and the Grenadines*

St. Vincent and the Grenadines enacted its revised Electronic Transactions Act (ETA) in 2015.[103] The ETA: provides that E-documents may be used to comply with provision of information, access to information, delivery of information, originality of documents, or document retention requirements; states that E-documents are admissible evidence in a court of law; established E-contract rules relating to contract formation, time and place of dispatch and receipt, use of automated message rules, and errors; contains a third-generation E-signature law; creates requirements for secure E-signatures and E-documents; contains rules for licensing and regulation of Information Security Procedure Providers; provides fundamental rules of E-government concerning provision of information to citizens; contains rules for E-commerce sellers and internet service providers; contains extensive consumer protections for E-commerce buyers, allowing the buyer to cancel an E-contract at any time within 10 days after receipt of the goods or services; and states that violations of the ETA may result in a maximum penalty of a $250,000 fine and five years' imprisonment if the defendant is a person, but for business firms the maximum penalty is a $500,000 fine plus 10 percent of the firm's annual revenue.[104]

5.20. Trinidad and Tobago

The Electronic Transactions Act (ETA) was enacted in 2011.[105] The ETB contains a third-generation E-signature law. The ETB's remarkable aspects include numerous types of the fulfillment of statutory requirements using the electronic form; assumption that an E-signature supported with an accredited certificate has reliability and integrity; *prima facie* liability of Certification Service Providers (CSP) for damages caused by reliance upon an accredited certificate that it has issued, or has guaranteed; the specific mention that clicking of an icon on a computer screen is an acceptable method of acceptance of an offer; E-contract between a person and an electronic agent; and required method of opting out of receipt of future "spam" by its recipient.[106] The Computer Misuse Act (CMA),[107] enacted in 2000, is impressive. This is not surprising because it was closely patterned after one of the world's best computer crimes laws Singapore's CMA.[108]

5.21. Turks and Caicos

Turks and Caicos enacted its Electronic Transactions Ordinance (ETO) in 2000 but revised it in 2014.[109] The ETO: recognizes the legal validity of E-signatures and E-documents and provides they can be used to comply with legal requirements for writing, delivery, signature, originality, and retention; contains E-contract rules relating to the formation, attribution, acknowledgment of receipt, and time and place of dispatch and receipt of the message; contains a third-generation E-signature law; provides for heightened legal status for secure E-signatures; provides for licensing and regulation of [110] Certification Service Providers; allows for the encryption of E-messages; and explains legal liability of internet service providers and E-sellers.

[97] Id.
[98] Commonwealth of Puerto Rico, ELECTRONIC GOVERNMENT ACT ("EGA"), Act No. 151 of 22 June 2004; http://www.oslpr.org/download/en/2004/0151.pdf.
[99] Id.
[100] Saint Christopher and Nevis, Electronic Transactions Act, Chapter 18.44, 2017; https://aglcskn.info/documents/Act17TOC/Ch%2018.44%20Electronic%20Transactions%20Act.pdf
[101] Id.
[102] Saint Lucia, Electronic Transactions Bill, 2007; https://issuu.com/amlregulator/docs/electronic_transactions_act_st_luci .
[103] St. Vincent and the Grenadines, Electronic Transactions Act, 2015; http://www.gov.vc/images/PoliciesActsAndBills/SVG_Electronic_Transactions_Act_2015.pdf.
[104] Id.
[105] Republic of Trinidad and Tobago, Electronic Transactions Act, 2011; http://www.ttparliament.org/legislations/a2011-06.pdf.
[106] Id.
[107] Republic of Trinidad and Tobago, COMPUTER MISUSE ACT ("CMA"), 2000; https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf.
[108] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993, revised 2007; https://sso.agc.gov.sg/Act/CMA1993.
[109] Turks and Caicos, Electronic Transactions Ordinance, 2014; https://fliphtml5.com/fizd/ooxd/basic.
[110] Id.

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

5.22. *U.S. Virgin Islands*

The U.S. Virgin Islands has enacted the U.S. Uniform Electronic Transactions Act (UETA) in its entirety.[111] The overriding majority of U.S. jurisdictions 45 states, the District of Columbia, and the Territories of Puerto Rico and the Virgin Islands have done so. The UETA contains a second-generation E-signature law. Accordingly, most types of E-signatures are legally recognized, provided they possess the four common trustworthiness attributes: uniqueness to the user; capability of verification; under the sole control of the user; and linked to the data in such a manner that if the data is changed, the signature is invalidated. If all four criteria are met, the E-signature will be enforceable.[112]

6. Jamaica's Electronic Transactions Act

Jamaica's Electronic Transactions Act (ETA) became effective on 2 April 2007.[113] The purposes of the ETA are to facilitate the growth of E-commerce by enabling security in online communiqués; promote public confidence in E-contracts and E-documents by facilitation of authentication and integrity of the electronic form; and promote the development of E-government.[114] The Minister of Commerce, Science, and Technology ("Minister") is responsible for the implementation of the ETA. The ETA applies to private parties and the government.[115] The electronic form cannot be used in creating the following types of documents: wills; transfers of real property or an interest thereof;[116] trusts; powers of attorney; and those pertinent to the Civil Procedure Rules or other rules of courts.[117]

6.1. Legal Recognition, Fulfillment of Statutory Requirements, and E-Government

The legal validity of information or its admissibility into evidence in court[118] may not be denied merely because it is in electronic form, or because it is merely incorporated by reference in an E-document (if the information is familiar to the other party and was accepted by him).[119] If a statute requires the production of a paper document to incur a legal right, that requirement will be deemed to have been met with production of an E-document to a private party, provided: (a) it is readily accessible and available for subsequent reference; and (b) the other party consents to the use of the electronic form.[120] If the government is to be the recipient of the E-document, there are additional requirements: (a) any E-document format requirements in existence must have been complied with, and (b) any required verification method must have been complied with.[121] If a statute requires the production of more than one copy of a paper document, that requirement will be deemed to have been met with the production of one E-document.[122] If a statute requires the presence of a handwritten signature to incur a legal right, that requirement will be deemed to have been met if an E-signature is attached to an E-document and: (a) a procedure is used to identify the subscriber and that he approves the information in the E-document; and (b) that procedure is reliable in consideration of the purpose of the communiqué.[123] If the E-signature is to be presented to the government and the government requires a specific form of technology to be used in the procedure, that requirement must also have been met.[124] If the E-signature is to be presented either to a private party or the government, an encrypted signature is preferred because it will offer a greater degree of security than an unencrypted one.[125] If a statute requires the production of a notarized paper document, that requirement will be deemed to have been met with the production of an E-document that has the following "attached to or logically associated" with the E-document: the subscriber's encrypted signature; a statement attesting to the subscriber's identity; a statement by the subscriber confirming that all obligations have been complied with under the notarization statute; and all information required to be included according to any other laws.[126] If a statute requires the production of an original paper document, that requirement is deemed to have been met with production of an E-document if: (a) the integrity[127] of the information is maintained; (b) it is readily accessible for subsequent reference; (c) if presented to the government, any format requirements and verification-of-receipt requirements have been complied with; and (d) if presented to a private party, that party agrees to the electronic form.[128] If a statute requires a paper to be stored for a specific period, that requirement will be deemed to have been met by storage of an E-document, provided: (a) the E-document is readily accessible for subsequent reference; (b) the retention method maintains the integrity of the information; (c) a record is made of the time/place of transmission and reception of the communiqué, and that information is available for reference; and (d) any legal requirement concerning the specific type of "data storage medium" to be used, has been complied

[111] 10 L.P.R.A. s 4081 et seq. (2007).
[112] Id.
[113] Jamaica, ELECTRONIC TRANSACTIONS ACT ("ETA"), 2006, effective 2 April 2007; https://moj.gov.jm/sites/default/files/laws/Electronic%20Transactions%20pgs.%201-34.pdf.
[114] ETA s 3.
[115] ETA s 32. Recently, the implementation of the ETA has been assigned to the new Ministry of Mining and Telecommunications; its website is at http://www.mmt.gov.jm .
[116] However, a deed may be delivered electronically. ETA s 16(2).
[117] ETA s 4 (Schedule).
[118] For the specific rules regarding the admissibility of E-documents or E-signatures into evidence, see ETA s 12.
[119] ETA s 6.
[120] ETA s 7(1)(a) and (c).
[121] ETA s 7(1)(b). The giving of an E-document from one private party to another, or to/from the government to a private party, might occur in the context of: making applications or claims, giving notices or requests, making declarations or objections, or issuing or lodging a certificate. ETA s 7(3).
[122] ETA s 7(4).
[123] ETA s 8(1)(a)-(b). This rule is applicable regardless of whether the statute creates an obligation to present a handwritten signature, or merely states consequences to be incurred if there is no handwritten signature. ETA s 8(4). If the E-signature is to be given to a private party, that party must have agreed to accept the E-signature instead of a handwritten one. ETA s 8(1)(d).
[124] ETA s 8(1)(c).
[125] An encrypted signature is: uniquely connected to the subscriber, and the subscriber is identified; created with the subscriber's private key, and the key is under his sole control; and linked to the information in the attached E-document so that any modification of the information will be obvious. ETA 8(2). An encrypted signature supported by a certificate issued in a foreign country also has legal validity in Jamaica. ETA s 8(5). However, these requirements do not impede the right of the subscriber to use other methods of verification of the subscriber's identity and his approval, or his right to show evidence of the unreliability of an encrypted signature. ETA s 8(3).
[126] ETA s 9.
[127] Factors to consider in determination of integrity are: whether the document is complete and unchanged, other than for normal endorsements which occur during communication;
[128] ETA s 10(1).the purpose of the production of the information; and any other relevant information. ETA s 19(2).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

with.[129] If a statute requires information in a paper document to be served upon a party, that requirement will be deemed to have been complied with if an E-document containing the information is sent to the party, if the party acknowledges its receipt.[130] If the government has created a specific form of paper document to be submitted to the government, the Minister may promulgate a regulation allowing a substantially equivalent electronic form to be used.[131] If a statute requires that payment must be paid by a citizen to the government, the Minister may promulgate a regulation allowing the payment to be paid electronically, and specifying the manner of payment and security measures to be used.[132]

6.2. Certification Service Providers: General

A Certification Service Provider ("CSP") is defined as "a person who issues certificates for electronic signatures[133] or provides to the public other services related to electronic signatures."[134] An "encrypted signature" is an "electronic signature that is encrypted through a private key or other encrypted signature creation device."[135] A certificate may be issued to a party using his pseudonym instead of his legal name.[136]

CSP's licensed in foreign countries are recognized in Jamaica, and the certificates they have issued have legal validity; this open-minded approach is a strength of the statute. ETA s 8(5). However, this liberal provision does not affect other statutes that may require E-documents to: be signed with an encrypted signature; use a unique method of identification of the information contained therein; or use a specific means of identification of the subscriber and that he approved the information contained in the E-document.[137]

6.3. Regulation of CSP's

CSP's are regulated by the Certifying Authority ("CA"). The CA is empowered to issue certificates; issue and control the use of key pairs, authorize the issuance of certificates by CSPs; authenticate certificates; provide applications programming interface, and provide time-stamping services for E-documents. Additionally, the CA is responsible for conducting investigations of CSPs, if necessary.[138]

6.4. Legal Liability of Subscribers, Relying Third Parties and CSP's

A subscriber is responsible for: ensuring the security of the private key; informing relying third parties if the security of the private key may have been compromised, or has been compromised; ensuring that all information in the certificate is accurate; and indicating whether his E-signature is made in a personal capacity or an official capacity.[139] A relying third party is responsible for: doing everything reasonable to confirm whether an encrypted E-signature is reliable, and doing everything reasonable to verify the information in the certificate and to comply with its stated limitations.[140] A CSP is responsible for: adhering to its stated standard operating procedures; ensuring that information in the certificates is accurate; and ensuring a relying third party can determine specific information from the certificate or otherwise (the CSP's name, whether the subscriber had possession of the private key at the time issuance of the certificate, whether the private key was valid during the period of validity of the certificate, method used to identify subscriber, limitations on purpose or value, expressed limitations of liability of the CSP, the method used by the subscriber to give notice of insecurity of private key, revocation procedures, and trustworthiness[141] of CSP's computer system).[142]

6.5. Legal Liability of Internet Service Providers

Internet service providers that merely disseminate material of third parties ordinarily have limited liability for the content of that material, unless they know, or should know, that such dissemination will result in legal liability.[143]

6.6. E-Contracts

All parties to a contract must voluntarily agree to use the electronic form; no party may be compelled to accept or send E-documents or an E-signature against his will.[144] Any of the default provisions of the ETA relating to E-contracts may be varied by agreement of the parties.[145] An offer and acceptance may be made electronically, a declaration of intention may be made electronically, and E-contracts are valid (regardless if one or both of the parties used an automated communications device).[146]

Comprehensive attribution rules have been adopted.[147] Comprehensive rules regarding a change or error in an electronic communiqué have been adopted: If the parties have agreed to use a specific security procedure to detect changes or errors in a transmitted E-document, and only one party used the procedure, and the other party would have detected the change or error if it had used the procedure, then the party that used the procedure may disavow the E-document and act as if had never been sent.[148] A party dealing with the automated communications device of another party who makes an error and thereby generates an undesired E-document, may

[129] ETA s 11(1). An agent may also be used to store the E-document. ETA s 11(2).
[130] ETA s 13(1). This does not affect other rules concerning the time allowed for the serving of the information. ETA s 13(2).
[131] ETA s 14.
[132] ETA s 15.
[133] An E-signature is defined as "information that—(a) is contained in, attached to or logically associated with, an electronic document; and (b) is used by a signatory to indicate his adoption of the content of that document." ETA s 2.
[134] ETA s 2.
[135] Id.
[136] ETA s 24.
[137] ETA s 8(6).
[138] ETA s 26.
[139] ETA s 22.
[140] ETA s 21.
[141] Factors involved in assessment of trustworthiness include: hardware and software systems, procedure for processing of applications for certificates, record-keeping procedures, and frequency and comprehensiveness of audits of the CSP. ETA s 23(2).
[142] ETA s 23(1).
[143] ETA s 25.
[144] ETA s 5(2). The determination as to whether a party has voluntarily agreed to use the electronic form is as follows: in the case of the government, there must be an express statement; in the case of private parties, the party's conduct as well as the "context and surrounding circumstances" will be considered. ETA s 5(3).
[145] ETA s 5(5). Just because a party agrees to use the electronic form with one contract does not imply that he agrees to use the electronic form in other contracts. ETA s 5(4).
[146] ETA s 16.
[147] ETA s 17.
[148] ETA s 18(1)-(2).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

disavow the E-document and is not bound by it if the device did not provide an opportunity for correction of the error, and at the time of discovery of the error, the party: (a) promptly informed the other party of the error and that he disavowed the E-document; (b) followed the reasonable directions of the other party to return or dispose of any consideration received as a result of the incorrect E-document, or if no such directions were given, to return or dispose of the consideration. If the aforementioned situations do not apply, then the change or error will be controlled by any applicable provisions in the contract between the parties, or if there are no such provisions, then by other laws.[149] Comprehensive rules pertinent to the acknowledgment of receipt have been adopted.[150] Comprehensive rules regarding time/place of transmission/receipt of the communiqué have been adopted.[151]

7. Recommendations for Improvement of Jamaica's Internet Law

7.1. Add: Mandatory E-Government

To reduce cost and to make governmental functions more convenient for citizens, E-government needs to be emphasized and mandated. By established deadlines, governmental departments should begin to convert to the provision of online services if possible. In Hong Kong, for example, a substantial number of government services may now be accessed online, e.g., the scheduling of an interview for a visa or the scheduling of a wedding before a public official. However, the best example for Jamaica to follow in the implementation of mandatory E-Government is Puerto Rico; its Electronic Government Act is exemplary.[152]

7.2. Add: Stringent Consumer Protections

Jamaica's ETA lacks consumer protections for E-commerce buyers. The Republic of Tunisia's statute can be used as a paragon for good consumer protections. That statute gives E-commerce buyers: (1) a "last chance" to review the order before it is entered into; (2) a 10-day window of opportunity to withdraw from the agreement after it has been made; (3) a right to a refund if the goods are late or if they do not conform to the specifications; and (4) no risk during the 10-day trial period after the goods have been received. As a result, Tunisians enjoy some of the best consumer protections in the world.[153]

7.3. Add: Reciprocal Recognition of Foreign CSP's and Certificates

Most international E-commerce laws now provide for various forms of legal recognition of foreign CSPs and certificates issued in foreign countries, but the ETA fails to do this. This is essential because E-commerce transactions often straddle international borders. Turkey's Electronic Signature Law is a typical example and can be used as a paragon.[154]

7.4. Add: Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology ("I.T.") Courts should be established as a court-of-first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field, and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of Nepal can be used as a paragon.[155]

7.5. Add: Recognition of Electronic Wills

The ETA excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature affixed to it to be enforceable. This exclusion should be eliminated. Electronically signed wills should be recognized.[156]

7.6. Add: Injection of Computer Virus Is a Felony

The ETA's computer crimes section is deficient. For example, "Intentional Injection of a Virus into a Computer System" should be added as a felony. This crime is especially heinous because of its potential for infliction of extreme damage to the Jamaican and world economies. The punishment should be stringent, as follows: first offense, mandatory ten years' imprisonment, without parole; second offense, mandatory twenty years' imprisonment, without parole; and third offense, mandatory life imprisonment, without parole.

8. Conclusions

E-commerce in the Caribbean Region has been growing in recent years, but some Caribbean nations have not been participating in this growth because their E-commerce laws need to be updated. The purpose of this article is to recommend a Jamaican statute and a Puerto Rican statute for use as models by other nations in the Region. Jamaica's Electronic Transactions Act (ETA) contains a third-generation E-signature law; all types of E-signatures are accepted, but preference is given the digital signature. The most distinguished sections of the statute about the comprehensive section about the use of the electronic form to satisfy statutory

[149] ETA s 18(3).
[150] ETA s 19.
[151] ETA s 20.
[152] Note 91 supra.
[153] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 2000, art. 25-37; http://www.bakernet.com.org. See Stephen E. Blythe, Note 73 supra.
[154] Republic of Turkey, ELECTRONIC SIGNATURE LAW, 2004, art. 14.
[155] Kingdom of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the *Nepal Gazette* on 18 March 2005; it is available at http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf . *See* Stephen E. Blythe, Note 44 supra.
[156] The traditional aversion to electronic wills is dissipating. In 2005, the U.S. State of Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature. *See* Chad Michael Ross, Comment, "Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will," 35 UNIVERSITY OF MEMPHIS LAW REVIEW 603 (2005).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

requirements; legal liability of Certification Service Providers (CSP), subscribers, and relying on third parties; and the extensive provisions pertinent to the effect of an error or omission occurring during an E-commerce communiqué. Perhaps the weakest parts of the ETA are the computer crimes section and the E-government section. The ETA could be improved by adding amendments that would: mandate E-government; provide stringent protections for E-commerce buyers; recognize foreign CSPs and foreign certificates; establish information technology courts; make the injection of a virus into a computer system a felony, and recognize the validity of electronic wills. Puerto Rico's Electronic Government Act (EGA) is exemplary because it: mandates the implementation of a comprehensive list of E-government services at the Government Portal; assigns one government agency the responsibility of implementation of E-government and gives it broad powers to achieve that goal; and establishes a long list of specific government services that government departments are required to provide citizens. The amended ETA and the EGA are recommended for adoption by other nations in the Caribbean Region.

References

Anguilla, *Electronic Transactions Act*, Chapter E38. Retrieved at: http://www.gov.ai/laws/E038- Electronic%20Transactions%20Act/ .

Antigua and Barbuda. (2013). *Electronic Transactions Act*. Retrieved at: http://laws.gov.ag/wp-content/uploads/2019/04/Electronic-Transactions-Act-2013.pdf.

Berman, A.B. (2001). International Divergence: The "Keys'"To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures. *Syracuse J. Int'l L. & Com.* 28, 125,143-44.

Bahamas, Commonwealth of the. (2003). *Electronic Communications and Transactions Act*. Retrieved from: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf.

Barbados. (2001). *Electronic Transactions Act*, Cap. 308B. Retrieved from: http://admin.theiguides.org/Media/Documents/Electronic%20Transactions%20Act.pdf.

Bermuda. (1999). *Electronic Transactions Act.* Retrieved from: http://www.bermudalaws.bm/laws/Consolidated%20Laws/Electronic%20Transactions%20Act%201999.pdf .

Blythe, S.E. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security. *Richmond Journal of Law and Technology* 11(2), 6.

Blythe, S.E. (2005). Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's "Most Wired" City. *N.C. J. L. & Tech*. 7, 1.

Blythe, S.E. (2006). Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security. *Proceedings of the Sixth Annual Hawaii International Conference on Business* (2006).

Blythe, S.E. (2006). Computer Law of Tunisia: Promoting Secure E-Commerce Transactions with Electronic Signatures. *Arab L. Q.* 20, 317-344.

Blythe, S.E. (2006). A Critique of India's Information Technology Act and Recommendations for Improvement. *Syracuse J. Int'l L. & Com.* 34, 1.

Blythe, S.E. (2006). Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access. *J. Internet L.* 10, 20.

Blythe, S.E. (2006). "Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-Commerce," J. *Islamic State Practices in Int'l L*. 2(2), 5.

Blythe. S.E. (2006). Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality. *Ohio No. U. L. Rev.* 33, 525-562 (2006).

Blythe, S.E. (2006). The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation. *Houston J. Int'l L.* 28(3), 573-661.

Blythe, S.E. (2006). South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga. *J. So. Pacific L.* 10(1).

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

Blythe, S.E. (2006). Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World," *Sri Lanka J. Int'l L.* 18.

Blythe, S.E. (2007). Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region. *Columbia J. East European L.* 1(1) 44-75.

Blythe, S.E. (2007). The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries. *J. Econ. & Admin. Sciences* 22(1),103 (2007).

Blythe, S.E. (2007). China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce. *Chicago-Kent J. Intellectual Prop*. 7, 1.

Blythe, S.E. (2007). Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions. *Info. & Comm. Tech. L.* 16(1), 47-71 (2007).

Blythe, S.E. (2007). Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions. *Barry L. Rev.* 8, 23.

Blythe, S.E. (2007). Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth with Secure Cyber-Transactions. *I.C.F.A.I. J. Cyber L.* 6(4) 8-33.

Blythe, S.E. (2008). Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce with Secure Cyber-Transactions. *Transnat'l L. & Contemp. Problems* 17(2), 361.

Blythe, S.E. (May, 2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E- Commerce via Greater Cyber-Security. *Armenian L. Rev.*

Blythe, S.E. (August, 2008). Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber- Security. *European J. L. & Econ*. 26(1), 75-103.

Blythe, S.E. (May, 2008). E-Signature Law and E-Commerce Law of the European Union and its Member States. *Ukrainian J. Bus. L.* 22-26.

Blythe, S.E. (2008). Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services. *Hamline L. Rev.* 31(2), 445-469.

Blythe, S.E. (2008). On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law. J. High Tech. L. 8(1).

Blythe, S.E. (2009). The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate. *Proceedings of the Annual International Conference on Global Business*, Dubai, United Arab Emirates.

Blythe, S.E. (2009). Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act. A book chapter in *Internet Policies and Issues*, Frank Columbus, Ed., Nova Science Publishers, Inc., New York NY USA.

Blythe, S.E. (2009). The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control. *Proceedings of the Tenth Annual Conference of the International Academy of African Business and Development*, Kampala, Uganda.

British Virgin Islands. (2019). *Electronic Transactions Act*. Retrieved from: https://bvi.gov.vg/sites/default/files/electronic_transactions_act_2019_1.pdf .

Cayman Islands. (2003). *Electronic Transactions Law*. Retrieved from: https://laws-in-force.judicial.ky/WebSearchFileView.aspx?fileView=E%5CElectronic%20Transactions%20Law%20(2003%20Revision).pdf

China, Hong Kong Special Autonomous Region. (2000). *Electronic Transactions Ordinance*, Ord. No. 1, s 2.

Chung, R.C.Y. (2003). Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America. *Asian-Pacific L. & Pol'y J.* 4, 442.

Dominica, Commonwealth of. (2013). *Electronic Transactions Act*. Retrieved from: http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf .

Dominican Republic. (2002). *Law No. 126-02 Concerning Electronic Commerce, Documents, and Digital Signatures.* Retrieved from: https://indotel.gob.do/media/5129/ley-no-126-02-ingles.pdf .

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

E-Commerce in Jamaica Goes Hyper-Local Finally? (April 9, 2020). *Silicon Caribe.* Retrieved from: https://www.siliconcaribe.com/2020/04/09/ecommerce-in-jamaica-goes-hyper-local-finally/ .

European Union. (1999). *Directive1999/93/EC of the European Parliament and of the Council of13December 1999 on a Community Framework For Electronic Signatures* (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12.

Fischer, S.F. (2001). California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, *B.U. J. Sci. & Tech. L.* 7, 229, 233.

Froomkin, A.M. (1996). The Essential Role of Trusted Third Parties in Electronic Commerce. *Or. L. Rev.* 75, 49, 58.

Grenada. (2013). *Electronic Transactions Act*. Retrieved from: https://gov.gd/sites/hop/files/Acts-SROs/2013/Act%20No.%2021%20of%202013%20Electronic%20Transactions.pdf

Hallerman, D. (June 1, 1999). Will Banks Become E-commerce Authorities? *Bank Tech. News*, 12. Hogan, T.C. (2000). Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business? *N.C. Banking Inst*. 4, 417, 424-25.

Jamaica. (2006). *Electronic Transactions Act*. Retrieved from: https://moj.gov.jm/sites/default/files/laws/Electronic%20Transactions%20pgs.%201-34.pdf .

Kennedy, E. (February 18, 2018). The State of E-Commerce in the Caribbean. *St. Lucia Star.* Retrieved from: https://stluciastar.com/state-e-commerce-caribbean/ .

Maharaj, V. (June 3, 2020). 4 Steps for Small Business Owners in the Caribbean to Utilize Online Shopping. *Alternative Concepts*. Retrieved from: https://www.acmarketingcaribbean.com/post/4-steps-for-small-business-owners-in-the-caribbean-to-utilize-online-shopping .

Montserrat. (2013). *Electronic Transactions Act*, Chapter 11.32. Retrieved from: http://agc.gov.ms/wp-content/uploads/Electronic-Transactions-Act.pdf .

Nepal, Kingdom of. (2005). Electronic Transactions Ordinance No. 32 of the Year 2061 B.S., s 60-71. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the *Nepal Gazette* on 18 March 2005.

Netherlands Antilles. (2000). *Electronic Contracts Act*. Retrieved from: https://www.uaipit.com/uploads/legislacion/files/0000000241_State%20Ordinance%20Agreements%20via%20Electronic%20Channels-Eng.pdf .

Poggi, C.T. (2000). Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation. *Va. J. Int'l L.* 41, 224, 250-51.

Pun, K.H., Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan. (2002). Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?, *Hong Kong L.J*. 32, 241, 256.

Roland, S.E. (2001). The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues? *Suffolk U. L. Rev*. 35, 625, 638-45.

Ross, C.M. (2005). Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will. *U. Memphis L. Rev*. 35, 603.

Saint Christopher and Nevis. (2017). *Electronic Transactions Act*, Chapter 18.44. Retrieved from: https://aglcskn.info/documents/Act17TOC/Ch%2018.44%20Electronic%20Transactions%20Act.pdf

Saint Lucia. (2007). *Electronic Transactions Bill*. Retrieved from: https://issuu.com/amlregulator/docs/electronic_transactions_act_st_luci .

Saint Vincent and the Grenadines. (2015). *Electronic Transactions Act*. Retrieved from: http://www.gov.vc/images/PoliciesActsAndBills/SVG_Electronic_Transactions_Act_2015.pdf .

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 7
July/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n7p4
Article: Research

 www.cpernet.org

Shefchik, C. (May 21, 2020). Caribbean E-Commerce Gets a Boost from Covid. *The BVI Beacon.* Retrieved from: https://www.bvibeacon.com/caribbean-e-commerce-gets-a-boost-from-covid/ .

Singapore, Republic of. (1993, revised 2007). *Computer Misuse Act*, Cap. 50A. Retrieved from: https://sso.agc.gov.sg/Act/CMA1993 .

Singapore, Republic of. (1998). *Electronic Transactions Act*, Cap. 88.

Smedinghoff, T.J. (1999). Electronic Contracts: An Overview of Law and Legislation. *PLI/P*, 564, 125.

Stern, J.E. (2001). Federal Legislation: The Electronic Signatures in Global and National Commerce Act. *Berkeley Tech. L.J*. 16, 391, 395.

Tang, D.K.Y. (1999). Electronic Commerce: American and International Proposals for Legal Structures. *Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries* 333 (Christopher McCrudden Ed.).

Trinidad and Tobago, Republic of. (2000). *Computer Misuse Act*. Retrieved from: https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf .

Trinidad and Tobago, Republic of. (2011). *Electronic Transactions Act*. Retrieved from: http://www.ttparliament.org/legislations/a2011-06.pdf .

Tunisia, Republic of. (2000). *Electronic Exchanges and Electronic Commerce Law*, art. 25-37.

Turkey, Republic of. (2004). *Electronic Signature Law*, art. 14.

Turks and Caicos. (2014). *Electronic Transactions Ordinance*. Retrieved from: https://fliphtml5.com/fizd/ooxd/basic .

United Nations, Commission on International Trade Law. (1996). *Model Law on Electronic Commerce with Guide to Enactment*, G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49.

United States of America, Department of Commerce, *Haiti—Country Commercial Guide, 2020*. Retrieved from: https://www.trade.gov/country-commercial-guides/haiti-ecommerce .

United States of America. (2007). 10 L.P.R.A. s 4081 et seq.

United States of America, Commonwealth of Puerto Rico. (June 22, 2004). *Electronic Government Act*, Act No. 151. Retrieved from: http://www.oslpr.org/download/en/2004/0151.pdf.

United States of America, State of Utah. (1999). *Utah Code Annotated* 46-3-101 *et seq*.

United States of America. (1998). *Uniform Commercial Code* Sect. 2-201, 2-209.

Weathers, F. (January 19, 2019). The Caribbean's First US$ 1 Billion Startup. *Medium.com.* Retrieved from: https://medium.com/gobeyond-ai/the-caribbeans-first-us-1-billion-startup-45863b6a00c5 .

Wright, B. (2001). Eggs in Baskets: Distributing the Risks of Electronic Signatures. *West L.A. L. Rev.* 32, 215, 225-26.

Zaremba, J. (2003). International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers. *Conn. J. Int'l L.* 18, 479, 512.