International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

Cambodia's New Digital Signature, E-Commerce and Consumer Protection Laws: Key Components of a Bold Strategy for Dramatic Future Economic Growth

Stephen Errol Blythe, Ph.D., Ph.D., J.D.
Associate Professor of Accounting and Business Law
Department of Accounting, Finance and Economics
College of Business
Tarleton State University
Stephenville and Fort Worth, Texas
Email: blythe@tarleton.edu
USA

ABSTRACT

Cambodia has a bold new strategy to stimulate E-commerce and to grow the economy. The Digital Signature (DSL), Consumer Protection (CPL), and E-Commerce Laws (ECL) are important components of that strategy. The DSL provides for licensing of certifying authorities and does not prohibit other types of E-signatures. The CPL prohibits deceptive advertising and creates a consumer complaint procedure. The ECL recognizes the legal validity of secure E-documents and E-signatures, including as evidence in a court of law. The ECL states requirements of secure E-signatures and secure E-documents; E-contract rules; rules for liability of internet service providers and E-sellers; E-government provisions; E-payments services rules; and computer crimes. The ECL should be improved by: (a) recognizing electronic wills, powers of attorney, and real estate documents; (b) adding attribution rules and acknowledge receipt rules for E-contracts; (c) adding mandatory E-government; (d) adding a comprehensive computer crimes law; and (e) adding IT Courts.

Keywords: Cambodia, law, E-commerce, digital, signature, consumer, protection

Objectives of the Article

The objectives of this article are to (1) consider recent E-commerce growth and development in Cambodia; (2) explain the roles of electronic signatures, cryptology, public key infrastructure, and certification authorities; (3) describe the three generations of electronic signature law; (4) concisely cover Cambodia's Digital Signature Law and Consumer Protection Law; and (5) analyze Cambodia's Electronic Commerce Law in some detail and make recommendations for its improvement.

Background: Recent Growth in Cambodian E-Commerce

Cambodia has a population of approximately 17.3 million and its real Gross Domestic Product has been growing at an annual rate of 7%.[1] Internet penetration has been growing steadily and is now over 40%.[2] In the last decade, Cambodia's financial technology sector has developed rapidly, making financial products and services more accessible to Cambodians. The growing popularity of smartphones connected to the internet has facilitated the proliferation of local E-commerce business firms and also enticed foreign E-commerce firms to enter the market.[3] E-commerce sales in 2021 are forecast to be the US $222 Million, with about half of the goods going to China. E-commerce sales are growing at an annual rate of 9% and are projected to be the US $313 Million in 2025.[4] To stimulate E-commerce growth even further, the government of Cambodia recently announced its visionary, comprehensive 30-year E-Commerce Strategy consisting of policy development and institutional coordination, laws, and regulations (including the new Digital Signature, E-Commerce, and Consumer Protection Laws, the focal point of this article), information and communications technology infrastructure, digital knowledge, payment systems, domestic e-commerce logistics, international trade, access to finance, and trade information and market support. That strategy has the lofty goal of transforming Cambodia into an upper-middle-income country by 2030 and a high-income country by 2050.[5]

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] U.S. Central Intelligence Agency, *CIA World Factbook*, "Cambodia," June 8, 2021; https://www.cia.gov/the-world-factbook/countries/cambodia/ .
[2] Id.
[3] Jay Cohen and Pichrotanak Bunthan, Tilleke & Gibbins Law Firm, "What Cambodia's New Law on Electronic Commerce Means for Business," *Lexology*, March 2, 2020; https://www.lexology.com/library/detail.aspx?g=442bd243-f5af-4002-a3b4-b4d8c4e24f39 .
[4] "Digital Markets: E-commerce, Cambodia," *Statista*; https://www.statista.com/outlook/dmo/ecommerce/cambodia
[5] Hin Pisei, "E-Commerce Strategy Launched," *Phnompenh Post*, November 25, 2020; https://www.phnompenhpost.com/business/e-commerce-strategy-launched .
[6] See, e.g., United States, *Uniform Commercial Code* Sect. 2-201, 2-209 (1998).

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

electronic data and which serve as a method of authentication."[7] An electronic signature may take several forms: a digital signature, a digitized fingerprint, a retinal scan, a PIN, 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]

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: (a) 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 (b) 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: (a) it verifies authenticity that the communication came from a designated sender; and (b) it verifies the integrity of the content of the message, giving the recipient assurance that the message was not altered.[18]

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

---

[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.
[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).

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

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]

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.

The Critical Role of the Certification Authority

For digital signatures to realize their 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 to judge whether they should place reliance on communications signed with a certain private key.[34]

[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.
[34] Note 29 supra at 426-27.

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

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]

Three Generations of Electronic Signature Law

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]

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.

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 statutory requirement that a pen-and-paper signature is affixed, it must be a digital signature created with PKI. Nevertheless,

[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] 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 Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

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 EuropeanUnion,[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]

Cambodia's Digital Signature Law

Cambodia enacted its Digital Signature Law in 2017.[71] The statute governs digital signatures, which are defined as "any data attached to the electronic message certifying the digital signatory and verifying the authentication of such electronic message signed by the digital signatory."[72] To be valid, the digital signature must have been issued by a Certified Authority (CA) or trust services provider licensed by the Ministry of Posts and Telecommunications of Cambodia (Ministry) and must certify the following: the signatory's identity, the authenticity of the mail attached to the digital signature, the date and hour the digital signature was signed, and the satisfaction of any other conditions required by the Ministry.[73]

This appears to be a Third Generation E-signature law because, although it does not explicitly recognize other E-signatures, neither does it state that other types of E-signatures are not recognized.[74]

This law does not consider whether cloud-based or remote E-signatures are acceptable. It also does not contain any provisions regarding data residency or the storage and processing of E-signature data in a foreign country. However, the law does state that a subscriber's private key may not be stored anywhere without written authorization from the owner of the digital signature certificate.[75]

The law does not contain any restrictions as to when digital signatures can be used. An E-document signed by an E-signature that is verified by a licensed CA has the same legitimacy as a signed paper document. A certified E-signature is also acceptable anytime a law requires a thumbprint, stamp, or name. This means, for example, that an electronic will could be signed with a certified digital signature.[76]

There are no special requirements or restrictions regarding the use of digital signatures in communication with government departments. However, the law does require online financial institutions to use only the digital signature; they cannot use other types of E-signatures.[77]

Cambodia's Consumer Protection Law

The Consumer Protection Law (CPL) was enacted on November 2, 2019, and went into effect immediately.[78]

Chapter 1: General Provisions

The CPL provides basic consumer protections, promotes fair competition, and applies to both brick-and-mortar business firms and E-sellers. The objective of the statute is to enable sellers and buyers to transact activities with trust. The term "consumer" refers to one who receives goods or services used primarily for personal, domestic, or household purposes and are not purchased for sale to others. "Consumer rights" refers to the right to access accurate information so that one can make the best possible purchasing decision, and the right not to be taken advantage of by fraudulent advertisements of sellers. "E-commerce" refers to the electronic trading of goods or services. "Unfair acts" include deceptive advertisements, misleading customers regarding terms of sale, failure to give relevant information to customers, and taking advantage of customers if the seller is aware that they are not in a position to protect their interests.[79]

Chapter 2: Implementing Institutions

The Ministry of Commerce's General Department of Consumer Protection is responsible for the implementation of

[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. Blythe, "The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries," 22:1 *J. 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] Royal Government of Cambodia, *Sub-Decree No. 246 on Digital Signatures*, 2017, cited in "Electronic Signature Laws & Regulations--Cambodia," *Adobe Sign*; https://helpx.adobe.com/sign/using/legality-cambodia.html .
[72] Id.
[73] Id.
[74] Id.
[75] Id.
[76] Id.
[77] Id.
[78] Royal Government of Cambodia, *Law on Consumer Protection* (CPL), 2019, English translation by Perfect Translation Services, Phnom Penh, Cambodia; https://ibccambodia.com/wp-content/uploads/2020/01/Law-on-Consumer-Protection_EN.pdf .
[79] CPL Chapter 1.

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

the CPL and will be advised by the National Consumer Protection Committee.[80]

Chapter 3: Consumer Associations

Consumers in each major sector of the economy may establish a consumer association by registering with the Ministry of Interior according to the Law on Associations and Non-Governmental Organizations. The association must next file the approved registration document and letter of authorization at the National Consumer Protection Committee.[81]

Consumer associations: (a) consult frequently with consumers; (b) act as a representative of consumers at the National Consumer Protection Committee or in a court of law; (c) represent consumers in public forums or with the press; (d) communicate with regulators regarding consumer policies; (e) creates a consumer protection working group in each sector; and (f) perform other duties assigned by the National Consumer Protection Committee.[82]

Chapter 4: Unfair Acts in Business

No business person is allowed to engage in unfair acts against consumers. Examples of unfair acts include deceptive advertising or sales promotions; misleading consumers regarding cost, price, or quantity of goods or services; using hard-to-read small print to make it difficult for consumers to understand the terms of an offer or sale; making unfound claims for self-defense to avoid liability; or failure to give consumers what was promised.[83]

Chapter 5: Unfair Practices

Generally, it is illegal for a seller to create consumer confusion in the purchase of goods and services. Furthermore, these specific types of unfair selling practices are prohibited: the deceptive promise of gifts and prizes; bait advertising; unfair solicitation sales; demanding or accepting payments without intention to supply goods or services according to the purchase order; false or misleading representations regarding some business activities; coercion by threat or force; pyramid schemes; and selling goods with a false trade description.[84]

Chapter 6: Information for Consumers

Sellers of goods and services must comply with regulations relating to minimum information requirements to be given to consumers. If there is any confusion as to the proper regulatory requirement, the National Consumer Protection Committee shall investigate the matter and seek a resolution. The minimum information given to consumers includes type, classification, safety, quantity, origin, usage function, maintenance, composition, design, installation, usage instruction, cost, packaging, promotion or supply, dates of manufacture and expiration, and production information or information related to the supply of goods or services.[85]

Chapter 7: Complaint and Investigation Procedures

The National Consumer Protection Committee (NCPC) is authorized to begin an investigation into a consumer-related matter on its initiative, or it may accept a complaint from another regulatory agency, consumer association, or person. If necessary, the NCPC may ask another regulatory agency to conduct the investigation.[86]

After receiving a complaint, the NCPC ordinarily will appoint an ombudsperson to investigate the matter. The ombudsperson must be a qualified judicial officer to determine whether any legal offenses have been committed. The ombudsperson has the following rights: investigate and gather pertinent evidence; inspect the goods or services in question; take a sample of other relevant products or tools; ask witnesses to provide answers to questions or to produce documents; and take action to temporarily ban the goods or services when they are not in compliance with the law.[87]

Chapter 8: Procedures for Issuance of Decisions

After an investigation, the NCPC is empowered to issue a decision and/or an administrative sanction. The NCPC may take into account any advice received from a competent regulatory agency. The NCPC may negotiate a settlement with the parties involved so long as no criminal laws have been violated. If there has been a criminal violation, the NCPC may order the dissemination of relevant information by the seller, or the NCPC may order the seller to correct any erroneous information that was previously disseminated by the seller. If a manager or director has twice (during five years) engaged in deceptive advertising, bait advertising, coercion, pyramid schemes, or other unfair practices against consumers, that manager or director will be prohibited from continuing to serve as a manager or a director for a period of 2 to 5 years.[88]

Chapter 9: Appeal of NCPC Decision

Any relevant person may file a complaint with the National Consumer Protection Committee, requesting that a decision be reviewed, corrected, or revoked within fifteen days. The complaint must allege the NCPC's decision was not based upon substantial evidence. After the NCPC has reviewed the initial decision and issued its final decision, the losing party may file a complaint in a court of law within 30 days.[89]

Chapter 10: Penalties

The sanctions provided in the CPL include a written warning, suspension, revocation, or cancellation of a certificate of commercial registration or license, obstruction penalty, fine, and imprisonment.[90]

Chapter 11: Final Provisions

Any previous law contrary to the CPL is superseded. The CPL became effective on November 2, 2019.[91]

[80] CPL Chapter 2.
[81] CPL Chapter 3.
[82] Id.
[83] CPL Chapter 4.
[84] CPL Chapter 5.
[85] CPL Chapter 6.
[86] CPL Chapter 7.
[87] Id.
[88] CPL Chapter 8.
[89] CPL Chapter 9.
[90] CPL Chapter 10.
[91] CPL Chapter 11.

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

Cambodia's Electronic Commerce Law

The Law on Electronic Commerce (ECL) was enacted on November 2, 2019. and went into effect on May 2, 2020.[92] The statute established a basic legal foundation for both domestic and international E-commerce transactions. It is a major component of the Cambodian government's long-range plan to stimulate E-commerce and to dramatically increase economic growth.[93]

Chapter 1: Purpose, Goals, Scope, Definitions of Terms

The ECL was enacted to provide basic rules for E-commerce transactions and to promote the utilization of electronic communication among Cambodians. Accordingly, the ECL has these objectives: (a) achievement of authenticity, accuracy, and reliability in electronic messaging; (b) development of a legal framework conducive to the proliferation of E-commerce; (c) reduction of computer hacking and viruses; (d) reduction of uncertainty in situations where E-documents and E-signatures are used in place of paper documents and handwritten signatures; (e) to promote E-government by allowing citizens to file E-documents with the government, and allowing government departments to fulfill notice requirements by servicing E-documents; and (f) to create rules and standards relating to authenticity and accuracy of E-documents.[94]

The ECL created three exceptions in which E-documents and E-signatures are not allowed: (a) creation or enforcement of a power of attorney; (b) creation or execution of a will; and (c) documents relating to the ownership, purchase, or sale of real property. In those situations, the electronic form cannot be used; paper documents and handwritten signatures are required. Unfortunately, the ECL carved out these exceptions and this needs to be rectified.

Definitions of key terms are listed in the attached glossary.

Chapter 2: Legal Validity of Electronic Form

The legal validity of the following is recognized: E-messages, E-documents, and E-signatures. In a court of law, they may not be objected to due to their electronic form.

If any provision of law requires a written document, that requirement may be met with an E-document. If any provision of law requires a handwritten signature, that requirement may be met with a secure E-signature. If any provision of law requires records to be retained in their original form, that requirement may be met with an E-document. If any provision of law requires information to be made available in any form, that provision shall be replaced with an E-document so long as the E-document contains most or all of the information, it is accessible or downloadable for later use, and it can be stored. If any provision of law requires records to be saved, that requirement may be met with E-documents if they may be accessed later, it is stored in its original form, and the source and the date creation of the information can be determined. A court of law cannot preclude evidence in electronic form merely because it is electronic or because it is not in its original form.[95]

E-contracts are legally valid. Notwithstanding the above provisions, the parties to a contract may implement activities differently and may agree not to use the electronic form or may impose additional requirements relating to the form and authenticity of the contract.[96]

Chapter 3: Electronic Communications Process

Information in an E-message shall be considered sent when it left the information system under the control of the sender; or, if the information has been transmitted but has not left the sender's information system, then it is considered sent whenever it has been received by the recipient. Information is assumed to have been sent from the sender's place of business. Information is assumed to have been received when it becomes available for download by the recipient, and the information is assumed to have been received at the recipient's place of business.[97]

A proposal in an E-message to enter into an E-contract, which is not addressed to a specific person, shall be considered only as an invitation to form a contract; it shall be considered to be an offer.[98] A contract between a natural person and an automated system, or a contract between two automated systems, cannot be objected to merely because of the absence of a natural person.[99]

Whenever a natural person gives incorrect information to an automated system and the automated system does not allow the natural person to correct the information, then the natural person is allowed to correct the information if: (a) the natural person promptly informed the other party of the error and proves that incorrect information was entered, and (b) the natural person does not benefit from the entering of the incorrect information before providing notice to the other party. If the transaction was for the sale or purchase of a security, this provision is inapplicable.[100]

Conspicuous by their absence are attribution rules and rules about the acknowledgment of receipt.

Chapter 4: Secure E-Signatures and Secure E-Documents

An E-document is considered secure only if specific security procedures have been applied to ensure that the E-document has not been altered during all relevant times.[101]

An E-signature is considered secure only if these conditions are met: (a) it is associated with only one

[92] Royal Government of Cambodia, *Law on E-Commerce* (ECL), 2019, English translation by Perfect Translation Services, Phnom Penh, Cambodia; http://www.perfecttranslationservices.com/en/news/law-on-e-commerce .
[93] "Law on Electronic Commerce Enacted in Cambodia," *Abacus IP: Cambodia*, November 6, 2019; https://www.abacus-ip.com/post/law-on-electronic-commerce .
[94] ECL Chapter 1.
[95] ECL Chapter 2.
[96] Id.
[97] ECL Chapter 3.
[98] Id.
[99] Id.
[100] Id.
[101] ECL Chapter 4.

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

subscriber; (b) it identifies only one subscriber; (c) it was created by the subscriber; (d) it indicates the date and hour of the signature; and (e) it describes the original condition of the E-message or E-document associated with that signature. These requirements do not limit the ability of any person in an E-message to require other conditions relating to the reliability of an E-signature or to prove that an E-signature is unreliable.[102]

Unless there is proof to the contrary, a secure e-document shall be assumed to have been unaltered from any specific time. Unless there is proof to the contrary, a secure E-signature shall be assumed to have been made by the relevant person, the relevant person affixed the signature to the E-document, and the relevant person approves the E-document to which it is affixed. If an E-document or an E-signature is not secure, then no assumptions regarding authenticity or accuracy shall be made.[103]

Identity theft is prohibited. No person shall use another person's E-message, E-document, E-signature, E-address, or password without authorization.[104]

Governance of security procedures relating to electronic messages, documents, and signatures is the responsibility of the Ministry of Posts and Telecommunications (Ministry).[105]

Chapter 5: Liability of Internet Service Providers and E-Sellers

Internet service providers and E-sellers do not have civil or criminal liability due to the information contained in an E-message if they did not send the E-message and: (a) they were not aware that the information sent could lead to legal liability; (b) they did not anticipate in advance the information could lead to legal liability; and (c) if they became aware afterward, they promptly removed the information, stored it and informed the Ministry. After investigation, the Ministry may order them to (a) remove the information; (b) stop providing or postpone all services, or (c) stop providing or postpone electronic services.[106]

Internet service providers and E-sellers are not responsible for monitoring information contained in an E-message and determining if it is legally acceptable. However, this does not relieve them from their responsibility to comply with laws and regulations, court orders, and contractual obligations.[107]

Internet service providers and E-sellers shall not have civil responsibility under a contract, or outside a contract, if they have complied in good faith with the orders of the Ministry. Persons making deceptive charges, not in good faith, against internet service providers or E-sellers shall bear civil or criminal responsibility.[108]

Internet service providers and E-sellers must have a license. The Ministry of Commerce issues licenses to E-sellers, both natural persons and legal entities. The Ministry of Posts and Telecommunications issues online service certificates to internet service providers.[109]

Internet service providers and E-sellers shall comply with the Code of Ethics issued by the two respective ministries.[110]

Chapter 6: Consumer Protection

An E-seller is required to provide honest information about its: (a) personal name or corporate legal name, personal address or registered; address; and email address or telephone number; (b) a fast, effective, and convenient method of communication; (c) terms, conditions of sale, payment methods, cancellation methods, how to replace goods, and refund procedure; and (d) the items which are available for sale. The information must be sufficient to enable the buyer to make a decision. The requirements in this paragraph are inapplicable to securities and the insurance industry.[111]

Any person or entity sending unsolicited business information or advertisement shall provide easy and convenient methods for the recipient to reject the communication.[112]

No person or entity shall create an electronic system designed to convey false information or to cause confusion to take advantage of, and cause damage to, the recipient of the information.[113]

No person or entity shall transmit a virus or inject a virus into another person's information system.[114]

Chapter 7: E-Government

Government agencies are now allowed to make online transactions, including (a) acceptance of filed documents from citizens, (b) issuing licenses and permits to citizens, and (c) acceptance of payments and fees from citizens. Additionally, government agencies are now allowed to store their records electronically.[115]

Chapter 8: Digital Evidence Rules

An E-document, E-message, or an E-signature cannot be rejected as evidence in a court of law merely because it is in electronic form or it is not in the original form.[116]

An E-document that has been printed from electronic records is admissible as evidence, provided that the document is duly printed per the original content.

If an E-document originated in a foreign country, the document may be admissible: (a) if it has been certified by the competent authority of the foreign country, and (b) the electronic system used to record or store the E-document is accurate under the standards established in the ECL.

[102] Id.
[103] Id.
[104] Id.
[105] Id.
[106] ECL Chapter 5.
[107] Id.
[108] Id.
[109] Id.
[110] Id.
[111] ECL Chapter 6.
[112] Id.
[113] Id.
[114] Id.
[115] *Abacus IP: Cambodia*, Note 79.
[116] Zico Law Firm, *ASEAN Insiders Series: Electronic & Digital Signatures in ASEAN*, December, 2020, p. 5; https://www.zicolaw.com/wp-content/uploads/2020/12/ASEAN-INSIDERS_Electronic-Signatures.pdf .

International Journal of Social Science and Public Policy *(IJSSPP)*

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Center for Promoting Education and Research (CPER) USA www.cpernet.org

Chapter 9: Electronic Payments and Fund Transfers

A payment system company is required to obtain prior authorization from the National Bank of Cambodia. Payment system firms' responsibilities and potential liability in case of fraud are enumerated. Customers are required to inform their payment service within two days of discovery.[117]

Chapter 10: Enforcement and Fines

Complaints may be filed with either the Ministry of Posts and Telecommunications of the Ministry of Commerce. Both of those agencies are authorized to levy a fine against violators of the ECL.[118]

Chapter 11: Sanctions

Both of the aforementioned ministries are authorized to issue the following penalties: (a) warning; (b) withdrawal of business license; (c) fine; and (d) imprisonment. This chapter also explains how to determine whether a business entity may be criminally liable, and the consequences.[119]

Chapter 12: Abrogation of Prior Conflicting Law, and Date of Effect

All prior laws in conflict with the ECL are superseded by the ECL. The ECL went into effect on May 2, 2020.[120]

Recommendations for Improvement of Cambodia's E-Commerce Law

Delete: Three Exceptions

The three exceptions (power of attorney, real property, and wills) listed in Chapter 1 of the ECL should be eliminated. In this age of Zoom teleconferencing, there is no good reason why a power of attorney and real estate sales documents cannot be authenticated digitally. Electronic will have been recognized in some jurisdictions for more than 15 years.[121]

Add: Attribution Rules

The U.N. Model Law on E-Commerce recommends the inclusion of attribution rules to determine the source of an E-message.[122] For an example, refer to Section 17 of Jamaica's Electronic Transactions Act.[123]

Add: Rules Pertaining to Acknowledgement of Receipt

The U.N. Model Law on E-Commerce also recommends the inclusion of rules pertaining to the acknowledgment of receipt of an E-message.[124] For an example, refer to Section 19 of Jamaica's Electronic Transactions Act.[125]

Add: Mandatory E-Government

Cambodia has established rudimentary rules for E-government, but they need to be expanded. To reduce costs and to make governmental functions more convenient for citizens, E-government should be mandated. By established deadlines, governmental departments should begin to convert to the provision of online services if possible. The best example for Cambodia to follow in the implementation of mandatory E-Government is Puerto Rico; its Electronic Government Act is exemplary.[126]

Add: Stringent Consumer Protections

Cambodia has established a basic foundation of protections for E-commerce buyers, but they need to be strengthened. 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.[127]

Add: Computer Crimes Law

Cambodia has recognized some basic computer crimes in the ECL, but a comprehensive computer crimes law is needed. Singapore's Computer Misuse Act is the best model to emulate.[128]

Add: Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology (IT) Courts should be established as a court-of-first-instance for them. The IT 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 IT 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 IT person would be required to hold a graduate degree in an IT-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.[129]

Conclusions

The Cambodian government has embarked upon a bold new plan to dramatically stimulate E-commerce and to grow the economy. Its recent enactment of the Digital Signature, Consumer Protection, and E-Commerce Laws are important components of that strategy. The Digital Signature Law (DSL) provides for the licensing of certifying authorities by the Ministry of Posts and Telecommunications. The DSL appears to be the Third Generation because it does not explicitly prohibit the use of other types of E-signatures. The

[117] *Abacus IP: Cambodia*, Note 79.
[118] Id.
[119] Id.
[120] Id.
[121] 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 *U. Memphis L. Rev.* 603 (2005).
[122] Note 46 *supra.*
[123] Jamaica, *Electronic Transactions Act*, 2006, effective 2 April 2007; https://moj.gov.jm/sites/default/files/laws/Electronic%20Transactions%20pgs.%201-34.pdf .
[124] Note 46 *supra.*
[125] Note 123 *supra*.
[126] Commonwealth of Puerto Rico, *Electronic Government Act*, Act No. 151 of 22 June 2004; http://www.oslpr.org/download/en/2004/0151.pdf .
[127] Republic of Tunisia, *Electronic Exchanges and Electronic Commerce Law*, 2000, art. 25-37.
[128] Singapore, Republic of. (1993, revised 2007). *Computer Misuse Act*, Cap. 50A. Retrieved from: https://sso.agc.gov.sg/Act/CMA1993 .
[129] 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.

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

Consumer Protection Law (CPL) creates basic consumer rights and is administered by the Ministry of Commerce's Department of Consumer Protection. The CPL applies to both brick-and-mortar sellers and E-sellers. Sellers are required to be honest, they are forbidden to use deceptive business methods, and a complaint and sanctions procedure is established. The E-Commerce Law (ECL) established the legal validity of a secure E-document and a secure E-signature and states that they may be used to comply with statutory requirements pertaining to a written document; a handwritten signature; retention of a document; retention of a document in the original form; availability and accessibility of a document; and evidence in a court of law. Requirements of secure E-signatures and secure E-documents are stated. Foreign Certified Authorities are recognized so long as their standards are comparable to those in Cambodia. Most E-contract rules are provided; conspicuous by their absence are attribution rules and rules pertaining to the acknowledgment of receipt. The ECL contains rules for the determination of liability of internet service providers and E-sellers. The ECL requires E-sellers to be honest in transactions with consumers. E-Government is mentioned only briefly; it is allowed but it is not mandated. Licensing, administration, and potential sanctioning of E-payments services is established. A list of computer crimes with maximum sanctions is included, but it needs to be expanded. The ECL should be improved by: (a) allowing the electronic form to be used in wills, powers of attorney, and in real estate transactions; (b) making E-contracts better by adding attribution rules and rules pertaining to acknowledge of receipt; (c) adding mandatory E-government to make government services more efficient and more convenient for citizens; (d) adding a comprehensive computer crimes law; and (e) adding Information Technology Courts.

References

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.

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).

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).

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

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.

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.

European Union. (1999). *Directive1999/93/EC of the European Parliament and of the Council of 13 December 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.

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*.

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.

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.

VOL: 3, ISSUE: 7
July/2021
https://ijssppnet.com/
E-ISSN: 2663-7200
DOI: 10.33642/ijsspp.v3n7p1

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.

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

Singapore, Republic of. *Electronic Transactions Act* (Cap. 88), 10 July 1998.

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.).

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

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, 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.

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.