JICLT
Journal of International Commercial Law and Technology
Vol. 9, No.4 (2014)

Fine-Tuning Vietnam's Electronic Transactions Law To Promote Growth in E-Commerce

Stephen E. Blythe
Professor of Accounting and Business Law,
College of Business Administration, Abu Dhabi University,
P.O. Box 59911, Abu Dhabi, United Arab Emirates
ecommercelaw@hotmail.com.

Abstract: In the digital age, the E-signature has replaced the handwritten signature. Since 1995, there have been three generations of E-signature law: the first mandated use of the digital signature, the second recognized the legal validity of all types of E-signatures, and the third recognizes all types of E-signatures, but gives preferred status to the digital signature. Vietnam's Electronic Transactions Law ("ETL"), enacted in 2005, is third-generation; it recognizes all types of E-signatures, but favors use of the digital signature. Accreditation requirements are specified for Certification Authorities ("CA"), the issuers of certificates and verifiers to third parties that a digital signature is that of a specific subscriber. The CA is responsible for maintaining the security of information that it receives from its subscribers. The CA must inform the subscriber of any limitations on the use of the certificate. If an accredited CA issues a qualified certificate, it must meet more stringent security requirements which can only be achieved with a digital signature. CA's must maintain a publicly-accessible repository of certificates and the public keys which relying third parties can use to decrypt a subscriber's message. A CA may incur legal liability for publishing a certificate with inaccurate information or for not issuing a private key to the subscriber corresponding to the public key in the repository. The ETL allows certificates issued by CA's in foreign countries to be recognized if they provide sufficient security. The author recommends that the following provisions be added to the ETL: (1) consumer protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; (5) explicit long-arm jurisdiction; and (6) recognition of legal validity of electronic wills.

1. Introduction

"Vietnam is a developing, mainly agrarian country that is moving from a centrally-planned economy to a market economy."1 More than 25% of all Vietnamese now have access to the internet.2 As more and more Vietnamese get online, E-commerce in Vietnam grows at an ever-expanding pace. In 2011, E-commerce sales were only about $350 million, but during 2012 they spiked to $500 million; that's a 43% increase. And in 2015, the E-commerce market is forecast to be $2.5 billion, a 500% increase in only three years.[3]

Despite these impressive numbers, E-commerce has been hampered by several factors: (a) the preference of Vietnamese to use cash instead of credit cards in transactions, and the reluctance of merchants to pay the 2% credit card fee; (b) more affluent persons in Vietnam are usually older and often not computer-literate, and younger Vietnamese are often more computer-literate but have less money to spend in E-commerce transactions; (c) wariness of many Vietnamese to purchase anything without seeing and touching it;[4] and (d) the failure of Vietnam's E-commerce law to meet the needs of E-commerce

[1] U.S. Department of State, Bureau of Consular Affairs, "Vietnam: Country Specific Information," 20 November 2012, p. 1; http://www.state.gov/r/pa/ei/bgn/3396.htm.
[2] U.S. Central Intelligence Agency ("CIA"), THE WORLD FACTBOOK, "Vietnam," 7 January 2013, pp. 3, 15; https://www.cia.gov/library/publications/the-world-factbook/geos/vm.html.
[3] Anh-Minh Do, "E-Commerce in Vietnam: A Status Report," Part 1, p. 1, ASIA E-COMMERCE, 13 December 2012; http://www.techinasia.com/ecommerce-vietnam-status-report-part-1/ .
[4] Id.

participants.[5] This article will address the last of those factors and will make recommendations for amendment and improvement of Vietnam's E-commerce law.

The objectives of this article are to: (1) recognize the significant growth trend in Vietnam's E-commerce and to point out several factors hampering this trend; (2) explain the role of electronic signatures, cryptology, public key infrastructure, and certification authorities; (3) describe the three generations of electronic signature law; (3) analyze Vietnam's Electronic Transactions Law ("ESL"); and (5) make recommendations for amendment and improvement of the ESL.

2. E-Signatures and the Advantages of the Digital Signature

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 "any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing,"[7] or as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[8]

An electronic signature may take a number of forms: a digital signature; a digitized fingerprint; a retinal scan; a scanned, digitized image of a handwritten signature attached to an electronic message; clicking the "I accept" or "I agree" icon (the "clickwrap" method); the name in a email address; a pin number; or merely a name typed at the end of an e-mail message.[9]

When entering into a contract online, four degrees of security are possible. In ascending order, they are: (1) merely clicking an "I Agree" button on a computer screen; [10] (2) the use of a password or a credit card number to verify a customer's intention that goods or services are to be purchased;[11] (3) use of a biometric method, a unique physical attribute of a party (e.g., a voice pattern, facial recognition, a scan of the retina or the iris within a person's eyeball, a digital reproduction of a fingerprint,[12] or a digitized image of a handwritten signature that is attached to an electronic message);[13] and (4) a digital signature, which is more complex and provides more security than biometrics.[14] Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the

---

[5] "E-Commerce Laws Need to be Amended," THE VOICE OF VIETNAM ONLINE, 26 August 2012, p. 1; http://english.vov.vn/Economy/Ecommerce-laws-need-to-be-amended/229266.vov.

[6] *See*, e.g., United States of America, UNIFORM COMMERCIAL CODE Art. 2-201, 2-209 (1998); http://www.law.cornell.edu/ucc/2/article2.htm.

[7] Thomas J. Smedinghoff, "Electronic Contracts: An Overview of Law and Legislation," 564 PLI/P at 125, 162 (1999).

[8] EUROPEAN UNION DIRECTIVE 1999/93/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; http://europa.eu/legislation_summaries/information_society/l24118_en.htm.

[9] David K.Y. Tang, "Electronic Commerce: American and International Proposals for Legal Structures," in REGULATION AND DEREGULATION: POLICY AND PRACTICE IN THE UTILITIES AND FINANCIAL SERVICES INDUSTRIES 333 (Chrisopher McCrudden ed., 1999); **and Stephen Mason, ELECTRONIC SIGNATURES IN LAW (3rd Edition, Cambridge University Press, 2012).**

[10] Jonathan E. Stern, Note, "Federal Legislation: The Electronic Signatures in Global and National Commerce Act," 16 BERKELEY TECHNOLOGY LAW JOURNAL 391, 395 (2001).

[11] Id.

[12] In the highly successful Hong Kong Identity Card, the two thumb prints are used as a biometric identifier. Rina C.Y. Chung, "Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America," 4 ASIAN-PACIFIC LAW AND POLICY JOURNAL 442 (2003).

[13] "The Legality of Electronic Signatures Using Cyber-Sign is Well Established," CYBER-SIGN; http://www.cybersign.com/news news.htm.

[14] 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;" and (2) The recipient of the document must have a database of biological traits of all signatories dealt with in order to verify that a particular person sent the document. 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 LAW JOURNAL 241, 256-57 (2002). The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers, but there are dissenters; e.g., see Benjamin Wright, "Symposium: Cyber Rights, Protection, and Markets: Article, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures,'" 32 WEST LOS ANGELES LAW REVIEW 215, 225-26 (2001).

case, however; the digital signature refers to the entire document.[15] 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."[16] 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.[17]

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI."[18] PKI consists of four steps. (1) A public-private key pair is created; the private key will be kept in confidence by the sender, but the public key will be available online. (2) The sender will 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. [19] (3)The digital signature is attached to the message and both are sent to the recipient. (4) The recipient will 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.[20]

3. Three-Generations of Electronic Signature Law

A. First Generation: Digital Signature Required

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[21] In the Utah statute, digital signatures were required and other types of electronic signatures were not recognized.[22] 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; other jurisdictions granting exclusive recognition to the digital signature include Argentina,[23] Bangladesh,[24] India[25], Malaysia,[26] Nepal,[27] New Zealand[28] and Russia.[29]

---

[15] 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." Hong Kong Special Autonomous Region, ELECTRONIC TRANSACTIONS ORDINANCE, Ord. No. 1 of 2000, s 2; http://www.hklii.org/hk/legis/en/ord/553/.

[16] Note 7 supra at 146.

[17] Christopher T. Poggi, "Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation," 41 VIRGINIA JOURNAL OF INTERNATIONAL LAW 224, 250-51 (2000).

[18] 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 BOSTON UNIVERSITY JOURNAL OF SCIENCE AND TECHNOLOGY LAW 229, 233 (2001).

[19] Pun, Note 14 supra at 249.

[20] Jochen Zaremba, "International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers," 18 CONNECTICUT JOURNAL OF INTERNATIONAL LAW 479, 512 (2003).

[21] UTAH CODE ANN. 46-3-101 *et seq.*, 1995. This first-generation statute was repealed in 2000 and replaced with the Uniform Electronic Transactions Act, a second-generation model law. UTAH CODE ANN. 46-4-101 *et seq.* (2000); http://le.utah.gov/~code/TITLE46/46_04.htm.

[22] Id.

[23] Argentine Republic, DIGITAL SIGNATURE DECREE 2628/2002, 19 December 2002; http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/80733/norma.htm . The original act was amended by DIGITAL SIGNATURE DECREE 724/2006 on 8 June 2006; http://infoleg.mecon.gov.ar/infolegInternet/anexos/115000-119999/116998/norma.htm . *See* Stephen E. Blythe, "A Critique of Argentine E-Commerce Law and Recommendations for Improvement," GOLDEN GATE UNIVERSITY ANNUAL SURVEY OF INTERNATIONAL AND COMPARATIVE LAW___(2011), published by Golden Gate University School of Law, San Francisco, California USA. Portions of that article was presented as a paper at the

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 possible disadvantages: more expense because of the fee paid to the certification authority; lesser convenience due to being forced to use a certification authority; forcing users to use one type of technology to the exclusion of others when another type of technology might be better suited to a particular type of transaction; use of a more complicated technology which may be less adaptable to technologies used in other nations, or even by other persons within the same nation; inappropriate risk allocation between users if fraud occurs; and the potential disincentive to invest in development of alternative technologies.[30]

B. Second Generation: All Types of E-Signatures Accepted

Jurisdictions in the Second Generation overcompensated. They did the complete reversal of the First Generation 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. The United States of America[31] is a member of this generation; the overriding majority of its jurisdictions (forty-five states, the District of Columbia, and the Territories of Puerto Rico and Virgin Islands) have enacted the Uniform Electronic Transactions Act (either in its entirety or with minor amendments), a permissive second-generation model law.[32] Australia has also enacted a second-generation statute.[33]

FOURTH INTERNATIONAL CONFERENCE ON GLOBAL STUDIES, Rio de Janeiro, Brazil, 18-20 July 2011, sponsored by Common Ground Publishing, Inc., University of Illinois Research Park, Champaign, Illinois USA.

[24] Bangladesh, INFORMATION TECHNOLOGY (ELECTRONIC TRANSACTION) ACT 2000 (Draft); http://www.bangladeshgateway.org/lawit.pdf .

[25] Republic of India, THE INFORMATION TECHNOLOGY ACT, 9 June 2000; http://www.mit.gov.in/itbillionline/itbill2000.asp. *See* Stephen E. Blythe, "A Critique of India's Information Technology Act and Recommendations for Improvement," 34 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 1 (2006), a publication of the College of Law, Syracuse University, Syracuse, New York USA.

[26] Republic of Malaysia, DIGITAL SIGNATURE ACT, 1997; http://www.mycert.org.my/bill/digisign/digi1.html .

[27] Federal Democratic Republic of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), ss 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; http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf. *See* Stephen E. Blythe, "On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law," 8:1 JOURNAL OF HIGH TECHNOLOGY LAW (2008), a publication of Suffolk University School of Law, Boston, Massachusetts USA.

[28] New Zealand, ELECTRONIC TRANSACTIONS ACT 2000; http://www.med.govt.nz/templates/ContentTopicSummary____9829.aspx.

[29] Russian Federation, ELECTRONIC DIGITAL SIGNATURE LAW, Federal Law No. 1-FZ, 10 January 2002; http://www.russoft.org/docs/?doc=166.

[30] Amelia H. Boss, "The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce," 34:3 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673, 689-90 (2009). It is debatable as to whether technological-neutrality or technological-specificity is the correct road to take. *See* 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 UNIVERSITY LAW REVIEW 625, 638-45 (2001).

[31] For analysis of American law, *see* Stephen E. Blythe, "E-Commerce and E-Signature Law of the United States of America," THE UKRAINIAN JOURNAL OF BUSINESS LAW, Kiev, Ukraine, November, 2008; http://www.ujbl.info/. For concise coverage of American, British, European Union and United Nations 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); http://law.richmond.edu/jolt/v11i2/article6.pdf.

[32] United States of America, National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 20 (Supp. 2000); http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm. The State of Washington is the only U.S. jurisdiction presently having a first-generation statute, and these states have third-generation statutes: Alabama, Georgia, Florida and Ohio. *See also* United States of America, ELECTRONIC SIGNATURES IN GLOBAL AND

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

C. Third Generation: Acceptance of All E-Signatures, With a Preference for Digital Signature

Singapore was the vanguard of the Third Generation. In 1998, that country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. In terms of relative degree of technological neutrality, Singapore adopted a "hybrid" model—a preference for the digital signature in terms of greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures.[34] The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in the original Utah statute. 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.[35]

In recent years, more and more nations have joined the Third Generation. 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 in order for an electronic record to comply with any statutory requirement that a record be in paper form; and (3) in order for a signature in electronic form to comply with a statutory requirement that a pen-and-paper signature be affixed, it must be a digital signature created with PKI. Nevertheless, the Third Generation jurisdictions do not appear to be as technologically-restrictive as those in the First Generation. They do not compel the E-commerce participant to use only the digital signature, *in lieu* of other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

NATIONAL COMMERCE ACT ("E-Sign"), Public Law 106-229, 15 U.S.C. 7001, 114 Stat. 464, 30 June 2000; http://www.esignrecords.org/resources/esign.pdf.

[33] Commonwealth of Australia, ELECTRONIC TRANSACTIONS ACT 1999; http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/.

[34] Singapore's lawmakers were influenced by the U.N. Model Law on E-Commerce. *See* 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); http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html. *See* Stephen E. Blythe, Note 31 supra, second citation.

[35] Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88), 10 July 1998, amended in 2010; http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_legdisp.pl?actno=2010-ACT-16-N&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%202010%0a&date=latest&method=part&sl=1.
Although granting legal recognition to most types of electronic signatures, the original Singapore statute of 1998 made 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 were given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carried a legal presumption of reliability and security—these presumptions were not given to other forms of electronic signatures; and (2) although all forms of electronic signatures were 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. *See* Stephen E. Blythe, "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33 OHIO NORTHERN UNIVERSITY LAW REVIEW 525-562 (2006). The ETA was amended in 2010 pertinent to: application and consent; electronic originals; time and place of dispatch and receipt; invitation to make offers; automated message systems; and E-government. Another amendment opens up the possibility of technological neutrality, i.e., that the ETA may eventually become applicable to other security procedures such as biometrics. Republic of Singapore, Infocomm Development Authority website, "Differences Between Electronic Transactions Act 1998 and Electronic Transactions Act 2010;" http://www.ida.gov.sg/Policies%20and%20Regulation/20100630114202.aspx. However, because the attainment of technological neutrality remains to be seen, the author declined at this point to reclassify Singapore as a member of the Second Generation.

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 United Nations' Model Law on Electronic Signatures,[36] the European Union's E-Signatures Directive,[37] Armenia,[38] Azerbaijan[39] Barbados,[40] Bermuda,[41] Bulgaria,[42] Burma,[43] China[44] Colombia,[45] Croatia,[46] Dubai,[47] Egypt,[48]

---

[36] United Nations Commission on International Trade Law: UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES WITH GUIDE TO ENACTMENT, ("MLES") 2001; http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html. The MLES takes an intermediate stance between two extreme positions: requiring the sole use of the digital signature (first generation), and acceptance of any type of E-signature (second generation). Instead, the MLES recognizes all types of E-signatures, but shows a preference for the digital signature. MLES comment 34.

[37] Note 8 supra; *see* Stephen E. Blythe, Note 31 supra, second citation. 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," THE UKRAINIAN JOURNAL OF BUSINESS LAW, pp. 22-26, May, 2008, Kiev, Ukraine. In an assessment of the effectiveness of its E-Signature Directive in 2006, the European Commission concluded that contracting parties had been slow to use digital signatures, but that "many other simpler electronic signature applications had become available." Reasons advanced by the Commission for the slow rate of adoption of digital signatures include: "technical problems in the marketplace, a lack of criteria for certification and mutual recognition, a lack of interoperability at national and cross-border levels, and the existence of isolated areas where certificates were used for a single purpose." Overall, the primary reason advanced was an economic one, caused by a typical user's decision to eschew development of a multi-application digital signature in favor of an E-signature which is applicable to its own industry, e.g., the banking sector. REPORT ON THE OPERATION OF DIRECTIVE 1999/93/EC ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES, s 5.2, COM (2006), cited in Boss, Note 30 supra at 695-96. Despite the less than enthusiastic reception of the digital signature in Europe and elsewhere, that rate of acceptance is expected to be given a "shot in the arm" felt worldwide by the "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (hereinafter "Rotterdam Rules");" http://www.unis.unvienna.org/unis/pressrels/2008/unisl125.html . The Rotterdam Rules became effective on 23 September 2009 and recognize the legal validity of electronic bills of lading. In order to comply with the security requirements of Article 38 of the Rotterdam Rules, it will apparently be necessary to employ a digital signature. Felix W.H. Chan, "In Search of a Global Theory of Maritime Electronic Commerce: China's Position on the Rotterdam Rules," 40 JOURNAL OF MARITIME LAW AND COMMERCE 185 (2009). *See also* Manuel Alba, "Electronic Commerce Provisions in the UNCITRAL Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea," 44 TEXAS INTERNATIONAL LAW JOURNAL 387 (2009). Accordingly, *a la* Mark Twain's rumored death, any notion that the digital signature is passé appears to have been "greatly exaggerated." The digital signature appears to have a bright future because, presently at least, it provides the epitome of security.

[38] Republic of Armenia, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2002; http://www.gipi.am/?i=223 . *See* Stephen E. Blythe, "Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security," ARMENIAN LAW REVIEW, May, 2008, a publication of the Department of Law, American University of Armenia, Yerevan, Republic of Armenia.

[39] Republic of Azerbaijan, THE LAW OF THE AZERBAIJAN REPUBLIC ON DIGITAL ELECTRONIC SIGNATURE, 2003; http://unpan1.un.org. *See* Stephen E. Blythe, "Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region," 1:1 COLUMBIA JOURNAL OF EAST EUROPEAN LAW 44-75 (2007), a publication of Columbia University School of Law, New York NY USA.

[40] Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B, 8 March 2001; http://www.barbadosbusiness.gov.bb/miib/Legislation/Acts/investment_acts.cfm. *See* Stephen E. Blythe, "The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute," 16 CARIBBEAN LAW REVIEW 1 (2006), a publication of the Faculty of Law, The University of the West Indies, Barbados.

[41] Commonwealth of Bermuda, ELECTRONIC TRANSACTIONS ACT 1999; http://www.bakernet.com/ecommerce/bermuda-eta.doc .

[42] Republic of Bulgaria, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2001; http://www.csd.bg/news/law/E-CommercePublE.htm. *See* Stephen E. Blythe, "Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions," 17:2 TRANSNATIONAL LAW AND CONTEMPORARY PROBLEMS 361 (2008), a publication of the University of Iowa College of Law, Iowa City, Iowa USA.

[43] The Union of Myanmar, ELECTRONIC TRANSACTIONS LAW, The State Peace and Development Council Law No. 5/2004, The 12 Waxing of Kason 1366 M.E., 30 April 2004; http://ibiblio.org/obl/docs/Electronic-transactions.htm. *See* Stephen E. Blythe, "Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As a Sign Of Hope For a Troubled Nation," 3:1 INTERNATIONAL BUSINESS RESEARCH __ (2010), a publication of the Canadian Center of Science and Education, Toronto, Canada; http://ccsenet.org/journal/index.php/ibr/ .

[44] People's Republic of China, Order No. 18 of the President, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, Promulgated 28 August 2004, Effective 1 April 2005. The statute was translated into English by the Beijing University School of Law, Beijing, China, and is available (by subscription only) at their website: http://www.lawinfochina.com/dispecontent.asp?db=1&id=3691. *See* Stephen E. Blythe, "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic

Finland,[49] Hong Kong,[50] Germany,[51] Hungary,[52] Iran,[53] Jamaica,[54] Japan,[55] Jordan,[56] Lithuania,[57]

Future Growth of E-Commerce," 7 CHICAGO-KENT JOURNAL OF INTELLECTUAL PROPERTY 1 (2007), a publication of Chicago-Kent College of Law, Illinois Institute of Technology, Chicago, Illinois USA. *See also* Felix W.H. Chan, "E-Commerce All at Sea: China Welcomes Digital Bills of Lading Under the Electronic Signature Law 2005," 3 OKLAHOMA JOURNAL OF LAW AND TECHNOLOGY 31 (2006).

[45] Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES, 13 January 1999, Official Translation No. 7 by Maria del Pilar Mejia de Restrepo; http://www.qmw.ac.uk/~t16345/colombia_en_final.htm. *See* Stephen E. Blythe, "Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act," published as Chapter 2 in PEER-TO-PEER NETWORKS AND INTERNET POLICIES, D. Vergos and J. Saenz, Editors, © 2010 Nova Science Publishers, Inc., Hauppauge, New York USA; ISBN: 978-1-60876-287-3; available for purchase at www.novapublishers.com.

[46] Republic of Croatia, ELECTRONIC SIGNATURE ACT, 17 January 2002; http://www.ehrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/00/document/eSignatureActOG10_2002.pdf. *See* Stephen E. Blythe, "Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security," 26: 1 EUROPEAN JOURNAL OF LAW AND ECONOMICS 75-103 (August, 2008), a publication of Springer Netherlands Ltd., Amsterdam.

[47] Emirate of Dubai, LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE NO. 2/2002, 12 February 2002; http://www.tecom.ae/law/law_2.htm. *See* 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 JOURNAL OF ECONOMICS AND ADMINISTRATIVE SCIENCES 103 (2007).

[48] Arab Republic of Egypt, LAW NO. 15/2004 ON E-SIGNATURE AND ESTABLISHMENT OF THE INFORMATION TECHNOLOGY INDUSTRY DEVELOPMENT AUTHORITY (ITIDA), 2004; http://www.uneca.org/aisi/NICI/Documents/egypt-e-signature-law.doc. *See* Stephen E. Blythe, "E-Commerce Security in the Land of the Pharoahs: Refining Egypt's Electronic Signature Law," 21:1 INDIANA INTERNATIONAL AND COMPARATIVE LAW REVIEW __(2011), a publication of the School of Law, Indiana University—Indianapolis, Indianapolis, Indiana USA; to become available at Lexis-Nexis and Westlaw.

[49] Republic of Finland, Ministry of Justice, ACT ON ELECTRONIC SIGNATURES, 2003; http://www.finlex.fi. *See* Stephen E. Blythe, "Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services," 31:2 HAMLINE LAW REVIEW 445-469 (2008), a publication of Hamline University School of Law, St. Paul, Minnesota USA.

[50] Hong Kong Special Autonomous Region, People's Republic of China, ELECTRONIC TRANSACTIONS ORDINANCE, Ordinance No. 1 of 2000. In the original statute, Hong Kong only recognized digital signatures and was therefore a member of the First Generation. After amendments were enacted in 2004, Hong Kong had a Third Generation statute; http://www.ogcio.gov.hk/eng/eto/download/es12004081114.pdf. *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 NORTH CAROLINA JOURNAL OF LAW AND TECHNOLOGY 1 (2005), a publication of the University of North Carolina School of Law, Chapel Hill, NC USA.

[51] "A Critique of the German Electronic Signature Law and Recommendations for Improvement," a paper presented and published in the PROCEEDINGS OF THE ACADEMIC AND BUSINESS RESEARCH INSTITUTE INTERNATIONAL CONFERENCE, San Antonio, Texas USA, March 22-24, 2012; http://www.aabri.com/SA2012.html.

[52] Republic of Hungary, ACT XXXV of 2001 ON ELECTRONIC SIGNATURE, 2001; http://www.techlawed.org. *See* Stephen E. Blythe, "Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions," 16:1 INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 47-71 (2007), a publication of Routledge Publishing Co., a member of the Taylor & Francis Group. Executive Editor: Prof. Indira Carr, Centre for Legal Research, Middlesex University, London, U.K.

[53] Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN; http://irtp.com/laws/ec/IR%20Iran%20E-Commerce%20Law.pdf. *See* Stephen E. Blythe, "Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World," 18 SRI LANKA JOURNAL OF INTERNATIONAL LAW (2006), a publication of the University of Colombo Faculty of Law, Colombo, Sri Lanka.

[54] Jamaica, ELECTRONIC TRANSACTIONS ACT, Act 15 of 2006; http://www.our.org.jm/index.php?option=com_content&view=article&id=761:the-electronic-transaction-act-act-15-2006&catid=123:act&Itemid=390 *See* Stephen E. Blythe, "Internet Law As A Potential Catalyst For Growth Of Caribbean E-Commerce: Jamaica's Statute As A Model," a paper presented and published in the READINGS BOOK OF THE ACADEMY OF BUSINESS ADMINISTRATION GLOBAL TRENDS CONFERENCE, Cancun, Mexico, December 19-22, 2009.

[55] Japan, LAW CONCERNING ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES, promulgated 24 May 2000, effective 1 April 2001; http://www.meti.go.jp/english/report/data/gesignconte.html. *See* Stephen E. Blythe, "Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access," 10 JOURNAL OF INTERNET LAW 20 (2006), Aspen Publishers, Inc., New York, NY USA.

[56] Hashemite Kingdom of Jordan, ELECTRONIC TRANSACTION LAW NO. 85 OF 2001; http://www.cbj.gov.jo/uploads/Electronic_Transactions_Law.pdf. *See* Stephen E. Blythe, "E-Commerce Security in the Hashemite Kingdom: Calibrating Jordan's Electronic Transactions Law," ADVANCES IN

Pakistan,[58] Peru,[59] Slovenia,[60] South Korea,[61] Taiwan,[62] Tunisia,[63] Turkey,[64] United Arab Emirates,[65] Vanuatu[66] and in the proposed statute of Uganda.[67] Many other nations have adopted the hybrid

---

COMMUNICATIONS AND MEDIA RESEARCH, Vol. 8, Chapter 5, Anthony V. Stavros, Ed., © 2011 Nova Science Publishers, Inc., Hauppauge, New York USA. ISBN: 978-1-61324-794-5; available for purchase at www.novapublishers.com.

[57] Republic of Lithuania, LAW ON ELECTRONIC SIGNATURE, No. VIII—1822 (July 11, 2000), As Amended, No. IX—934 (June 6, 2002); http://www3.lrs.lt/cgibin/preps2?Condition1=204802&Condition2. *See* Stephen E. Blythe, "Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions," 8 BARRY LAW REVIEW 23 (2007), a publication of Dwayne O. Andreas School of Law, Barry University, Orlando, Florida USA.

[58] Islamic Republic of Pakistan, ELECTRONIC TRANSACTIONS ORDINANCE, 2002; http://unpan1.un.org/groups/public/documents/apcity/unpan010245.pdf. *See* Stephen E. Blythe, "Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce," 2:2 JOURNAL OF ISLAMIC STATE PRACTICES IN INTERNATIONAL LAW 5 (2006), a publication of ElectronicPublications.org Ltd., Stockport, U.K. Editors: Prof. Javaid Rehman, School of Law, Brunel University, West London, U.K.; and Dr. Amir Ali Majid, School of Law, London Metropolitan University, London, U.K.; http://electronicpublications.org/catalogue.php?id=46 .

[59] Republic of Peru, LAW REGULATING DIGITAL SIGNATURES AND CERTIFICATES, 28 May 2000, translated by National Law Center for Inter-American Free Trade; http://natlaw.com/interam/ar/ec/tn/tnarecl.htm. *See* Stephen E. Blythe, Note 44 supra, second citation.

[60] Republic of Slovenia, Centre for Informatics, ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT, 2000; http://e-uprava.gov.si/eud/e-uprava/en/ECAS-Act-in-English.pdf. *See* Stephen E. Blythe, "Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions," 6: 4 THE I.C.F.A.I. JOURNAL OF CYBER LAW 8-33 (2007), a publication of ICFAI University Press, Institute of Chartered Financial Analysts of India, Hyderabad, India.

[61] Korean Legislation Research Institute, DIGITAL SIGNATURE ACT NO. 5792, *Statutes of the Republic of Korea,* Vol. 16 (II), pp. 1217-1220 (1999). The statute has been amended two times: (1) Act No. 6360 of 16 January 2001; and (2) Act. No. 6585 of 31 December 2001. *See* 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 JOURNAL OF INTERNATIONAL LAW 573-661 (2006), a publication of the University of Houston Law Center, Houston, Texas USA.

[62] Republic of China, ELECTRONIC SIGNATURES ACT, 2002; http://law.moj.gov.tw/Eng/Fnews/FnewsContent.asp?msgid=944&msgType=en&keyword. *See* Stephen E. Blythe, "Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security," a paper presented and published in the PROCEEDINGS OF THE SIXTH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON BUSINESS, Honolulu, Hawaii USA, May 25-28, 2006.

[63] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 9 August 2000; http://www.bakernet.com.org. *See* Stephen E. Blythe, "Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures," 20 ARAB LAW QUARTERLY 317-344 (2006), a publication of Brill Academic Publishers, Leiden, The Netherlands.

[64] Republic of Turkey, ELECTRONIC SIGNATURE LAW, 2004; http://www.tk.gov.tr/eng/pdf/Electronic_Signature_Law.pdf. *See* Stephen E. Blythe, **"**Improving Cyber-Security in Turkey Via Refinement of E-Commerce Law," 28:1 INTERNATIONAL JOURNAL OF MANAGEMENT __ (2011), published in Dorset, England, U.K.; http://www.intjnlmgmt.aol. *See also* Stephen E. Blythe, "Improving Cyber-Security in the Crossroads of Eurasia: Refining Turkey's E-Commerce Law," PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON BUSINESS MANAGEMENT, Lahore, Pakistan, 5-6 January 2011; sponsored by: School of Business and Economics, University of Management and Technology, Lahore, Pakistan; Instituteof Administrative Sciences, University of the Punjab; Sukkur Institute of Business Administration; and Association of Management Development Institutions in South Asia; http://www.umt.edu.pk/icobm/.

[65] United Arab Emirates, FEDERAL LAW NO. (1) OF 2006 ON ELECTRONIC COMMERCE AND TRANSACTIONS, 30 January 2006; http://www.tra.ae/pdf/legal_references/Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf. *See* Stephen E. Blythe, "Fine-Tuning the E-Commerce Law of the United Arab Emirates: Achieving the Most Secure Cyber Transactions in the Middle East," 1:4 JOURNAL OF INTERNATIONAL BUSINESS AND SOCIAL SCIENCE (2010)," published by the Centre For Promoting Ideas, Dhaka, Bangladesh; http://www.ijbssnet.com/. *See also* Stephen E. Blythe, "The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate," a paper presented and published in the PROCEEDINGS OF THE ANNUAL INTERNATIONAL CONFERENCE ON GLOBAL BUSINESS, Dubai, United Arab Emirates, May 10-13, 2009.

[66] Republic of Vanuatu, ELECTRONIC TRANSACTIONS ACT (Act. 24 of 2000) ("ETA"); http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/eta2000256.html. The E-commerce law of the Commonwealth of Bermuda was used as a model for this statute. "Vanuatu E-commerce," LOWTAX, p. 1; http://www.lowtax.net/lowtax/html/jvaecom.html. For a discussion of the ETA by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—*see* Hon. Prime Minister Barak T. Sope Maautamate, MP, Government of the Republic of Vanuatu, "The e-Business Act of 2000, The International Companies (E-Commerce

approach; Vietnam is one of them.

4. Vietnam's Electronic Transactions Law

Vietnam enacted its Electronic Transactions Law (hereinafter "ETL")[68] in 2005[69] and it became effective on 1 March 2006.[70] The purpose of the ETL is.[71] The ETL contains third-generation E-signature provisions and is technologically neutral.[72] The Ministry of Post and Telematics ("Ministry") is responsible for implementation of the ETL.[73] The ETL is inapplicable to documents pertinent to: real property; wills; marriage and divorce; birth and death; and bills of exchange.[74]

A. Fulfillment of Statutory Requirements

The legal validity of electronic information cannot be denied merely because of its form;[75] furthermore, electronic information cannot be denied admission into evidence merely because of its form.[76] Information in digital form may be used to satisfy a statutory requirement for the information to be: expressed in a paper document;[77] expressed in the original form;[78] or retained.[79] An E-signature may be used to comply with a statutory requirement for a paper document to be signed,[80] or to comply with a statutory requirement for a paper document to be stamped with a seal of a "concerned agency or organization."[81]

Amendment) Act of 2000, The Companies (E-Commerce Amendment) Act of 2000: A Plain English Explanation," pp. 3-7; http://www.vanuatu.gov.vu/government/library/Explanation%20of%20the%20ecommerce%20acts.htm. *See also* Stephen E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga," 10: 1 JOURNAL OF SOUTH PACIFIC LAW (2006), a publication of the School of Law, University of the South Pacific, Emalus Campus, Port Vila, Republic of Vanuatu.

[67] Republic of Uganda, ELECTRONIC SIGNATURES ACT, Draft, 2004; http://www.sipilawuganda.com/downloads/electronic%20signatures%20bill%202004.pdf. *See* "The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control," Special Edition: Issues in African Business Policies, 11:5 JOURNAL OF MANAGEMENT POLICY AND PRACTICE (ISSN No. 1913-8067), a publication of North American Business Press, Inc., West Palm Beach, Florida USA, 2010; available for purchase at: www.na-businesspress.com. Portions of this article were presented and published in the PROCEEDINGS OF THE TENTH ANNUAL CONFERENCE OF THE INTERNATIONAL ACADEMY OF AFRICAN BUSINESS AND DEVELOPMENT, Kampala, Uganda, May 19-23, 2009.

[68] National Assembly of the Socialist Republic of Vietnam, LAW ON E-TRANSACTIONS ("ETL"), 29 November 2005; http://mic.gov.vn/lawfiles/1355073.doc.

[69] ETL art. 54.

[70] ETL art. 53.

[71] ETL art. 1**.** If any other law is in contravention of this statute, the ETL will be controlling. ETL art. 3.

[72] ETL art. 5(3).

[73] ETL art. 8(2).

[74] Id.

[75] ETL art. 11.

[76] ETL art. 14(1). Factors to be considered in assignment of the weight of the evidence include: the reliability of the manner of its creation, transmission and storage; the measures taken to ensure that the evidence has not been modified since its creation; and the means of identification of its creator. ETL art. 14(2).

[77] ETL art. 12. The information must be accessible for subsequent reference. Id.

[78] ETL art. 13. The information must not have been modified, other than endorsements ordinarily occurring during transmission and reception; and it must be accessible for subsequent reference. Id.

[79] ETL art. 15. The information must be: accessible for subsequent reference; stored in the original format, or expressed in a format which is a truthful depiction of the contents; and the time and place of transmission and reception must be indicated. Id.

[80] ETL art. 24(1). This is allowed, provided: the subscriber's identity is indicated, as well as his approval of the document's contents; and the method of generation of the E-signature is "sufficiently reliable," given the context in which the document was created and transmitted. Id.

[81] ETL art. 24(2). This is allowed if the advanced E-signature of the agency or organization is used, and the E-signature is supported with a CA's certificate. Id.

B. Definitions

An E-signature consists of "words, letters, numerals, symbols, sounds or other forms," is created using "electronic means" and is "logically attached or associated with a data message and capable of certifying the person who has signed it as well as the approval of such person to the content of the signed data message."[82] A "secure" E-signature must be supported with a certificate issued by a CA.[83]

C. Certification Authorities

Vietnam's ETL is the only statute this researcher has found in which a CA is referred to as an "e-signature certification service-providing organization."[84] The primary duty of CA's is to issue certificates in support of advanced E-signatures.[85] CA's are categorized as "public" or "specialized."[86] CA's must: provide certification services in compliance with the ETL; use reliable equipment and competent personnel; guarantee the substantive portions of certificates they issue; facilitate ascertainment of origin of E-documents and attached E-signatures by relying third parties and state agencies; maintain an up-to-date and accessible registry of certificates; keep all relevant parties informed of the status of issued certificates; give all relevant parties at least ninety days' notice of intention to go out of business; and archive certificates for at least five years after cancellation.[87] The subscriber is responsible for: maintaining security of the private key; promptly informing the CA and relying third parties if the security has been compromised; and ensuring that truthful information is given to the CA and that the information contained in the certificate is accurate.[88] Relying third parties are responsible for: confirmation that the E-signature is reliable before accepting it; ascertainment of the validity of the supporting certificate, if any; and abiding by any limitations expressed in the certificate.[89] Certificates issued by foreign CA's are legally recogized in Vietnam if they have a comparable degree of reliabilty.[90]

D. E-Contracts

The legal validity of a contract cannot be denied merely because it is in electronic form.[91] However, all parties to a contract must have voluntarily agreed to use the electronic form; no one can be compelled to use it against his will.[92] E-contracts are controlled both by the ETL and by the law of contracts.[93] The parties are free to make agreements concerning "technical requirements, certification, and conditions to ensure integrity and confidentiality…"[94]

---

[82] ETL art. 21(1).
[83] ETL art. 22(2). Furthermore, an advanced E-signature: must be generated with signature creation data which are unique to the subscriber, and under his exclusive control at time of execution; and any subsequent modifications to either the E-signature or the attached document must be detectable. ETL art. 22(1).
[84] ETL art. 4(13). A CA is defined as "an organization carrying out e-signature certification services in accordance with the provisions of law." Id.
[85] A certificate must contain: name and contact information of CA and subscriber; identification number; period of validity; public key; CA's E-signature; limitations on purpose or value of transactions, if any; and limitations on CA's legal liability, if any. ETL art. 29.
[86] ETL art. 30. A public CA serves parties engaged in public activities, and a license is not required for them. ETL art. 30(2). On the other hand, a specialized CA serves parties engaged in "specialized activities or domains," and those CA's must hold a license. ETL art. 30(3).
[87] ETL art. 31(1). The Ministry is authorized to promulgate additional regulations pertinent to CA's. ETL art. 32(2).
[88] ETL art. 25(2).
[89] ETL art. 26(2).
[90] ETL art. 27(1). Factors to be used in determination of reliability include nternational standards; and treaties entered into by Vietnam. Id.
[91] ETL art. 34. An E-contract may be consummated either wholly or partially using the electronic form; an offer, acceptance or both may use the electronic form. ETL art. 36. This provision achieves one of the aims recently stated by the United Nations Commission on International Trade Law (UNCITRAL): if a nation's law provides that a contract must be in writing to be enforceable, that law may be satisfied if a contract is in electronic form. UNCITRAL, United Nations Convention on the Use of Electronic Communications in International Contracts (2005), art. 8(1); http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.
[92] ETL art. 35(1).
[93] ETL art. 35(2).
[94] ETL art. 35(3).

The attribution rules refer to the person himself or to an automatically-programmed computer, but do not include the agent of the person.[95] The rules relating to the time of receipt of the message are confusing because, at one point, they do not include the case where the recipient has not designed a computer system;[96] at another point, however, provision is made for both cases (i.e., in which the recipient has/has not designated a specific computer information system for the message to be sent).[97] Ordinary acknowledgement-of-receipt rules are included.[98] The rules relating to place of transmission and reception specify: an organization's place of business which is most related to the transaction in question; or in the case of an individual, his private residence.[99]

As a general rule, it is illegal for a person, agency or organization to violate the ETL; penal or administrative sanctions may be imposed.[100] More specifically, it is illegal to: prevent voluntary selection of the electronic form; interfere with transmission or reception of E-messages, or to modify them without authorization; create or sell software designed to sabotage a computer information system; use an E-message to commit another unlawful act; or to wrongfully use another's E-signature.[101]

Parties with disputes pertinent to E-contracts are encouraged to use mediation and conciliation instead of the court system, but the court system is available to resolve them if necessary.[102]

E. e-Government

A state agency may use the electronic form for communication: within itself; between itself and another agency; or between itself and an external private party.[103] State agencies are encouraged to use the electronic form and to prepare a plan for adoption of the electronic form.[104] State agencies are mandated to specify: the format and forms of E-messages to be used; types of E-signatures and certification requirements; and required security [105]procedures to be adhered to.[106] If a state agency's computer information system makes an error, the agency is responsible for promptly informing the other party and for correcting it.[107] The other party is also responsible for complying with the ETL and with state agencies' regulations relating to E-government.[108]

F. Security Obligations of the Parties

All parties engaged in an E-contract, or engaged in a communique with a state agency, are obligated to: use effective security procedures;[109] ensure that they do not contaminate the integrity of other parties' E-documents; [110] and maintain confidentiality of other parties' information.[111] Furthermore, an internet service provider ("ISP") has a duty to "prevent and stop the use of their network services for dissemination of data messages which are against the cultural traditions, national ethics, or prejudicial to the national security, public order and safety or violate other provisions of law;"[112] if the ISP fails to promptly remove offensive material after being instructed to do so by "competent state agencies," the ISP will be legally accountable.[113] This is an unfortunate provision because it forces internet service providers to look for and remove offensive materials, and there is a chilling effect on freedom of speech and the

[95] ETL art. 16.
[96] ETL art. 18(2)(a).
[97] ETL art. 19(1).
[98] ETL art. 18(2)(c)-(e).
[99] ETL art. 19(2).
[100] ETL art. 50. No penalties are specified for these offenses; this is a weakness of the statute.
[101] ETL art. 9. No penalties are specified for these offenses; this is a weakness of the statute.
[102] ETL art. 52.
[103] ETL art. 39.
[104] ETL art. 40(3)-(4).
[105] State agencies must be able to provide a high degree of security of their E-messages. ETL art. 41.
[106] ETL art. 40(6).
[107] ETL art. 42.
[108] ETL art. 43.
[109] ETL art. 44.
[110] ETL art. 45.
[111] ETL art. 46.
[112] ETL art. 47(1).
[113] ETL art. 47(2).

freedom of the internet. These same "competent state agencies" may require a party to store an E-document the agency is scrutinizing, or to provide a passport or access to a computer system they are inspecting.[114] Those agencies have an unfettered right to search and seize computer systems and E-documents of private parties;[115] this is egregious and further chills freedom of speech and freedom of the internet.

G. Evaluation of the ETL

The Electronic Transactions Law ("ETL") contains the following noteworthy provisions: third-generation E-signature rules which allow recognition of all types of E-signatures, while encouraging the use of the digital signature because of its advantages; use of an E-signature to comply with a statutory requirement for affixation of a organizational seal on a paper document, thereby sidestepping this antiquated contractual requirement emanating from the Middle Ages; preeminence of the ETL over other laws relating to E-transactions (e.g., contract law) if there is a disagreement between the two, which attaches more significance to this statute and provides for resolution of a potential conflict of laws; distinction between public and specialized CA's, allowing specialists to handle more complex transactions relating to specific categories; specification of relying third parties' responsibilities, thereby placing parameters on the responsibilities of CA's and subscribers; the freedom of parties to an E-contract to make an agreement regarding technical and certification requirements, resulting in the parties being allowed to tailor a contract to fit their specific technical and certification needs; defining an E-contract as either wholly or partially in electronic form, thereby defining E-contracts broadly in order to extend the scope of this statute and its attendant advantages; and responsibilities of parties to E-government transactions, providing notice to users of E-government services of their responsibilities. The ETL's most glaring defect is the unfettered power given to government agencies to police the internet and E-messages, and the onus placed on an ISP to police the content of material that it disseminates; these are not surprising developments given the authoritarian government of Vietnam. Other weaknesses include: absence of a comprehensive list of computer crimes and penalties, increasing the likelihood that the statute will not be enforced; attribution rules fail to include an agent of a sender, an essential item given the fact that persons often employ agents to conduct their business; confusion regarding assumed time of receipt of an E-message, an important factor whenever time is of the essence; and, despite encouraging the use of conciliation in dispute resolution, failing to mention the specific conciliatory methods to be used. Some of these deficiencies would be addressed by adopting the amended recommendations for change, covered next.

5. Recommendations for Improvement of Vietnam's Cyber law

This section needs a short introduction. Describe the current status of cyberlaw and why it necessitates the following recommendations!

Vietnam has chosen to name its cyber statute "Electronic Transactions Law." In other words, the statute's professed scope is law pertaining to all aspects of online consummation of all transactions, including business transactions. In order to consummate online transactions most effectively and efficiently, it is necessary to make several additions to the existing law, as follows:

A. Add: Consumer Protections in E-Commerce Contracts

Consumer protections for those entering E-commerce contracts have been overlooked. As a model, Vietnam can look to the European Union's Directive on Consumer Rights.[116] Chapter I of the Directive

[114] ETL art. 48.
[115] ETL art. 49.
[116] DIRECTIVE 2011/83/EC of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance;

contains common definitions, such as "consumer" and "trader"; it also provides that the Directive's rules are applicable to all Member States, except in a few specified cases. Chapter II contains types of information required to be provided to consumers by all traders; Member States may impose more onerous information requirements. Chapter III contains information required to be given to consumers by E-commerce traders; it also regulates an E-commerce consumer's right of withdrawal (length of the withdrawal, procedure and effects of the withdrawal) and includes a standard withdrawal form. Chapter IV contains rules pertaining to delivery and passing of risk in contracts for the sale of goods; it also contains rules regarding costs for use of debit or credit cards, rules on telephone hotlines operated by traders, rules concerning additional payments, and rules on the use of pre-ticked boxes. Chapter V contains general enforcement provisions and a mandate that the Member States must implement the Directive by 13 June 2014.[117]

B. Add: Several New Computer Crimes

The following computer crimes should be recognized: (a) Unauthorized Access to Computer Material; (b) Unauthorized Tampering with Computer Information; (c) Unauthorized Use of a Computer Service; (d) Unauthorized Interference in the Operation of a Computer; and (e) Unauthorized Dissemination of Computer Access Codes or Passwords. The Singapore Computer Misuse Act is one of the most comprehensive computer crime statutues and can be used as a model.[118]

C. Add: Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology Courts similar to those used in Nepal should be established as courts-of-first-instance for them. Nepalese I.T. Courts use tribunals comprised of three experts. The chairperson is an attorney versed in E-commerce law, and the other two members are an I.T. expert and a business management expert. The attorney is required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person is required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert is required to hold a graduate degree in business administration and have managerial experience.[119]

D. Add: Mandatory E-Government

In order 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 provision of online services if possible. Estonia has one of the world's best models of E-government. The country has established a national E-government portal. Government departments use online procurement. Many online services are provided to Estonians, including: filing of court documents; business registration; land registration; notary; administration of the the national I.D. card; and appointments with public officials.[120]

E. Add: Explicit Long-Arm Jurisdiction

Because so many of the E-transactions will occur between Vietnam residents and foreign parties, it would be prudent for Vietnam to formally state its claim of "long arm" jurisdiction against any party who is a

---

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:01:EN:HTML.

[117] European Commission, Justice, Consumer and Marketing Law, "The Directive on Consumer Rights," 16 July 2013; http://ec.europa.eu/justice/consumer-marketing/rights-contracts/directive/index_en.htm.

[118] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993, available at http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A. *See* Stephen E. Blythe, Note 35 supra.

[119] 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; http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf. *See* Stephen E. Blythe, Note 27 supra.

[120] Estonia, Centre of Registries and Information Systems, "E-governance in Estonia;" http://www.egov-estonia.eu/ .

resident or citizen of a foreign country, so long as that party has established "minimum contacts" with Vietnam.[121] Minimum contacts will exist, for example, if a cyber-seller outside of Vietnam makes a sale to a party living within Vietnam. In that situation, the E-contract rules of the ETL should be applicable to the foreign person or entity outside of Vietnam because that person or firm has had an effect upon Vietnam through the transmission of an electronic message that was received in Vietnam. The foreign party should not be allowed to evade the jurisdiction of the Vietnamese courts merely because they are not physically present in the country. After all, E-commerce is an inherently international phenomenon.

Vietnam should make treaties with other nations that account for most of its foreign E-commerce; the purpose of the treaties would be to establish reciprocal recognition of jurisdiction over E-commerce parties, and the enforcement of judgments in E-commerce lawsuits.[122] Also, Vietnam should become a member of the International Consumer Protection and Enforcement Network, an organization which identifies and promotes measures for effective consumer protection enforcement.[123] These actions should stimulate the growth of Vietnamese E-commerce because all parties will have a better means of dispute resolution.

F. Add: Recognition of Legal Validity of Electronic Wills

Vietnam should work toward minimization, if not elimination, of the ETL's exclusions from coverage. The country should begin this task by recognizing the legal validity of electronic wills. Presently, a will must be in paper form with a handwritten signature to be enforceable. This exclusion should be eliminated; electronically-signed wills should be recognized.[124]

6. Summary and Conclusions

Since 1995, there have been three generations of E-signature law: the first mandated use of the digital signature, the second recognized the legal validity of all types of E-signatures, and the third recognizes all types of E-signatures, but gives preferred status to the digital signature.

The Electronic Transactions Law ("ETL") includes a third-generation E-signature law and has the following noteworthy provisions: recognition that an E-signature may be used to comply with a statutory requirement for a paper document to be stamped with the seal of a "concerned agency or organization;" a dichotomy of CA's as either "public" or "specialized;" a relatively greater amount of responsibility placed on relying third parties to confirm the reliability of an E-signature before accepting it; recognition that an E-contract is governed not only by the ETL, but also by the general contract law; freedom of the parties to an E-contract to make agreements regarding technical requirements, confidentiality, certification and integrity; recognition that a contract may be consummated either fully, or partially, in electronic form; encouragement of use of mediation in dispute resolution of E-contracts; and, if a government department's computer system makes an error in a transaction or communiqué with a citizen, that department is responsible for informing the citizen and correcting the error. Unfortunately, the ETL has at least two weaknesses: several exclusions from coverage; and an egregious mandate for an internet service provider to police the internet and to remove any material which is contrary to national security, public order and safety, cultural traditions and national ethics. Undoubtedly, the latter item has a chilling effect on freedom of speech via the internet.

The following provisions are recommended to be added: (1) consumer protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; (5) explicit long-arm jurisdiction; and (6) recognition of legal validity of electronic wills.

---

[121] The Republic of Tonga is an example of a nation that has claimed long-arm jurisdiction over E-commerce parties, and its statute may be used as a model. *See* Stephen E. Blythe, Note 66 supra, final citation.

[122] U.S. Department of State, Bureau of Consular Affairs, "Enforcement of Judgments," 2013; http://travel.state.gov/law/judicial/judicial_691.html.

[123] "Member Countries," International Consumer Protection and Enforcement Network, 2013; http://www.econsumer.gov/english/members/overview.shtm.

[124] The aversion to electronic wills is beginning to dissipate. 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).

.* * * * *

Cite as: Blythe, S. , Fine-Tuning Vietnam's Electronic Transaction s Law to Promote Growth in E-Commerce. *Journal of International Commercial Law and Technology,* Vol. 9 No.4 (Nov, 2014)