Fine-Tuning the E-commerce Law of the United Arab Emirates: Achieving the Most Secure Cyber Transactions in the Middle East

Stephen E. Blythe
Professor of Law, School of Management,
New York Institute of Technology, CERT Technology Park,
P.O. Box 5464, Al Muroor Road, Abu Dhabi, United Arab Emirates.
E-Mail: itlawforever@aol.com, Phone: (971) (2) 404-8606

Abstract

The first objective is to give a brief description of the evolution of electronic signature ("E-signature") law. There have been three generations of E-signature law since the first E-signature statute was enacted in 1995. These three successive generations emphasized, respectively: exclusive recognition of public key infrastructure ("PKI") technology and the digital signature; technological neutrality, with all types of E-signatures and technologies recognized; and a hybrid perspective which recognized all types of E-signatures, with a preference shown for PKI in admission of E-signatures and electronic documents ("E-documents") into evidence. The second objective is to cover the major points of the Electronic Commerce Law ("ECL") of the United Arab Emirates ("UAE"). The ECL's distinguishing attributes include: a convenient specification in its Preamble of all other statutes affected by it; a statement that any issues not addressed by the ECL are controlled by other bodies of law; its definition of a secure E-document; a provision that international contracting parties may agree to use a specific Certification Service Provider ("CSP"), or to use a specific category of CSP's; provisions concerning electronic contracts ("E-contracts") automatically made by pre-programmed computers; the mandatory deportation of a foreign citizen convicted of a computer crime; and the provision that invocation of a penalty for a computer crime will not prevent a more stringent penalty from being imposed pursuant to another law. The third objective is to make recommendations for refinement of the ECL: (1) deletion of all exclusions from coverage (except for negotiable instruments); and (2) addition of: consumer protections, several new computer crimes, mandatory E-government, information technology courts, and explicit long-arm jurisdiction of those courts.

Key Words: UAE, E-commerce, E-signature, PKI, computer, law

1. Introduction

The United Arab Emirates enacted its first federal E-Commerce Law in 2006. This paper will include a brief background of the evolution of E-signature law, an evaluation of the UAE statute, and recommendations for its improvement.

2. The First Generation of E-Signature Law: Technological Exclusivity

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law (Utah, 1995). In the Utah statute, digital signatures using PKI technology were given legal recognition, but other types of electronic signatures were not.

The authors of the Utah statute believed, with some justification, that digital signatures and PKI technology 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 and PKI include Bangladesh, India (Blythe, 2006), Malaysia, Nepal (Blythe, 2008) and Russia (Fischer, 2001).

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 (Roland, 2001).

3. The Second Generation of E-Signature Law: Technological Neutrality

Jurisdictions in the Second Generation overcompensated. They did the complete reversal of the First Generation and did not include any technological restrictions 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 E-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 E-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 (Blythe, 2005 and 2008), the United Kingdom (Blythe, 2005 and 2008) Australia and New Zealand (Fischer, 2001).

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 (Blythe, 2009).

4. The Third Generation of E-Signature Law: A Hybrid

Singapore was in the vanguard of the Third Generation. In 1998, this country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce (United Nations, 1996). In terms of relative degree of technological neutrality, Singapore adopted a "hybrid" model—a preference for the digital signature and PKI in terms of 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 was not granted a monopoly as in Utah. Singapore allows other types of E-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.

Although granting legal recognition to most types of E-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 E-signatures: (1) digital signatures employing PKI are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and E-documents signed with them carry a legal presumption of reliability and security—these presumptions are not given to other forms of E-signatures; and (2) although all forms of E-signatures are allowed to be used in Singapore, its E-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 (Singapore, 1998).

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 PKI technology 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 an E-signature to comply with a statutory requirement for a handwritten signature to 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 E-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 E-signature law. The hybrid approach is the one taken by: the European Union's E-Signatures Directive (European Union, 1999); Armenia (Blythe, 2008); Azerbaijan (Blythe, 2007); Barbados (Blythe, 2006); Bermuda (Fischer, 2001), Bulgaria (Blythe, 2008); China (Blythe, 2007); Colombia (Blythe, 2009); Croatia (Blythe, 2008); Dubai (Blythe, 2007); Finland (Blythe, 2008); Hong Kong (Blythe, 2005); Hungary (Blythe, 2007); Iran (Blythe, 2006); Japan (Blythe, 2006); Lithuania (Blythe, 2007); Pakistan (Blythe, 2006); Peru (Blythe, 2009); Slovenia (Blythe, 2007); South Korea (Blythe, 2006); Taiwan (Blythe, 2006); Tunisia (Blythe, 2006); Vanuatu (Blythe, 2006); and in the proposed statutes of Uganda (Blythe, 2009). Many other nations are either currently using the hybrid approach or are considering the adoption of it; the United Arab Emirates is one of them.

5. The E-Commerce Law of the United Arab Emirates

The UAE joined the Third Generation of E-signature law when it enacted its Electronic Commerce Law ("ECL") in 2006. The introduction of the ECL is noteworthy because it lists all of the prior statutes which are affected by it (ECL, Preamble). The objectives of the ECL are to promote E-commerce and to facilitate its growth via creation of a legal framework (ECL art. 3). The ECL is implemented by the Ministry of Economy & Planning ("Ministry"), which is empowered to promulgate regulations to that effect (ECL art. 35). The ECL is inapplicable in the following situations: marriage and divorce; wills; real property deeds; transfer of real property; negotiable instruments; and required notarization (ECL art. 2(2)).

Accordingly, electronic documents cannot be used in those situations. If the ECL does not address a specific matter, that matter is controlled by international business law and "general principles of civil and commercial practice" (ECL art. 2(1)).

An E-signature is defined as "any letters, numbers, symbols, voice or processing system in electronic form applied to, incorporated in, or logically associated with a data message with the intention of authenticating or approving the same" (ECL art. 1). A "secure" E-signature is one in compliance with the requirements specified in ECL art. 18 (ECL art. 10(3)-(4) and art. 17(1)). Those requirements are: the E-signature is supported by a certificate issued by a CSP; and the E-signature and its certificate are reliable (ECL art. 18(3)). Furthermore, a secure E-signature must: be unique to its subscriber; identify the subscriber; be generated using a procedure under the sole control of the subscriber; and be linked to the E-document so that any subsequent alternation of the E-document leads to an invalidation of the E-signature. There is a rebuttable presumption that a secure E-signature: has been attached by the purported subscriber; confirms the subscriber's agreement with the contents of the E-document it is attached to; is reliable; and has not been modified since its generation. A "secure" E-document has had agreed-to or "commercially reasonable" authentication procedures applied to it to ensure it has not been modified. Factors to consider in determination of whether the procedures are commercially reasonable include: the characteristics of the transaction; the parties' experience and skill in dealing with similar transactions; the cost and availability of alternate procedures; and the procedures ordinarily used in the course of business for this type of transaction (ECL art. 16(2)).

The legal validity of an E-message cannot be contested merely because of its electronic form; furthermore, it is acceptable for an E-message to incorporate other information by reference so long as the information is retrievable (ECL art. 4). An E-document or E-signature may not be denied admission into evidence merely because of its electronic form; if these are the best evidence, they may not be denied admission merely because they are not original or in original form. Factors to consider in weighing electronic evidence include: the reliability of methods used in its generation or processing; the degree of maintenance of its integrity; and the reliability of its source or creator, if known (ECL art. 10). If a statute requires the storage of information in a paper document, that requirement will be deemed to have been met if it is stored in an E-document. However, there are provisions, as follows. The information must be: stored in the same format as the paper document, or in a format which accurately depicts the information; accessible for subsequent reference; and the time and place of transmission and reception must be indicated.

It is not necessary to store endorsements automatically generated during the ordinary course of sending and receiving. An agent may be used to store the E-documents. If a statute requires specific procedures to be followed, or a specific agent to be used, those requirements must be obeyed (ECL art. 5). Production of an E-document may be used to comply with a statutory requirement for production of a paper document; for this to happen, the provisions mentioned in ECL art. 5(1) must be complied with (ECL art. 7). An E-document may be used to comply with a statutory requirement for production or retention of a paper document in its original form. There are provisions: "reliable assurance" that the information in the E-document has not been altered, and ability to access it for subsequent reference (ECL art. 9).

A secure E-signature attached to an E-document may be used to comply with a statutory requirement for a handwritten signature on a paper document (ECL art. 8). A CSP is "an accredited or authorized person or organization that issues electronic attestation certificates. A certificate must contain: the name of the CSP; the name of the subscriber; a statement that the private key was operational at the time of issuance to the subscriber; any limitations of liability of the CSP; and any limitations on purpose or value of transactions (ECL art. 21(3)). A CSP also provides other services in this connection and in relation to E-signatures regulated by this law (ECL art. 1).

CSP's are regulated by the Certification Services Controller ("Controller") (ECL art. 20)). CSP's are mandated to hold a license and to perform these duties: use reasonable care to ensure the accuracy of information in certificates; maintain a website which enables relying third parties to obtain relevant information; establish a procedure which enables subscribers to inform all relevant parties of the compromise of the security of the private key, and to revoke the certificate; use a trustworthy computer information system; maintain adequate capitalization; and use sound auditing procedures (ECL art. 21(1)-(2) and art. 22). A certificate issued by a foreign CSP (and the E-signature supported by that certificate) is legally valid in the UAE if the requirements for its issuance are equivalent to the UAE, and the practices of the foreign CSP are as reliable as those of domestic CSP's. However, the contracting parties are free to specify the use of a particular CSP or category of CSP's.This agreed specification will be deemed enforceable in the UAE, unless this would be contrary to UAE law (ECL art. 23(1)-(6)).

CSP's are responsible for ensuring all information contained in the certificate is correct, and are legally liable to subscribers or relying third parties who are damaged thereby; however, CSP's are not liable if any limitations stated in the certificate were violated, or they are able to prove that they were not negligent (ECL art. 21(4)-(5)). Subscribers must: maintain security of the private key; promptly inform all relevant parties if the private key's security has been compromised, or there is a substantial risk of compromise; and ensure that all information contained in the certificate is accurate (ECL art. 19). Relying third parties must take reasonable action to verify the validity of the certificate, its current status, and any limitations on purpose or value; furthermore, they assume the risk that a certificate has been forged if reliance on the certificate is not reasonable under the circumstances (ECL art. 18(2) and (4)).

All parties to a contract must agree to use the electronic form; its use is not compulsory. However, consent to use of the electronic form may be inferred by a person's conduct (ECL art. 6(1)). A contractual offer and acceptance may be made electronically, and an E-contract is legally valid. Furthermore, a valid E-contract may be formed by the interaction of two automatically-programmed electronic agents, or by one person interacting with an automatically-programmed electronic agent (ECL art. 11). The ECL contains ordinary attribution rules (ECL art. 13) acknowledgement-of-receipt rules (ECL art. 14), and rules pertinent to time/place of transmission/reception of an electronic message (ECL art. 15). The aforementioned E-contract rules can be varied if all parties are in agreement (ECL art. 6(2)). Governmental departments are not mandated to use the electronic form; they must grant consent [ECL art.6(3)]. Governmental departments may accept or use the electronic form pertinent to filing or issuance of mandatory documents, payment of fees and tender and reception of bids (ECL art. 24(1)).

They may specific the manner and format of the citizens' electronic communiqués (ECL art. 24(2)). No one is allowed to publish a certificate in order to achieve a fraudulent purpose (ECL art. 25). The following acts carry criminal penalties: use of a certificate with knowledge that it contains inaccurate information (maximum penalty is one year's imprisonment and a fine of AED 250,000) (ECL art. 26); giving incorrect information to a CSP when applying for a certificate or in support of a request for suspension or revocation of a certificate (maximum penalty is six months' imprisonment and a fine of AED 100,000) (ECL art. 27); violation of a duty of confidentiality of information obtained pursuant to the ECL (maximum penalty is six months' imprisonment and a fine of AED 20,000, with an exemption allowed for required disclosure in a judicial proceeding or pursuant to the law) (ECL art. 28); and use of a computer to carry out an unlawful act which is specified in other laws (maximum penalty is six months' imprisonment and a fine of AED 100,000) (ECL art. 29).

If the crime is committed by a corporation, the entity is responsible as well as the corporate directors, managers or employees who have consented to it; the person may be imprisoned and fined not more than AED 100,000, and the entity may be ordered to pay an equivalent fine (ECL art. 10). All tools and devices used in commission of the crime may be confiscated (ECL art. 31). Foreign citizens committing these acts must be deported (ECL art. 32). These penalties, if invoked, will not prevent a more stringent penalty from also being invoked pursuant to another law (ECL art. 33).

6. Recommendations for Improvement of the ECL

The UAE has taken a commendable first step toward attainment of a sound E-commerce law. Although the ECL is a significant accomplishment, it has not gone far enough. The following amendments should be implemented:

a. Delete: All Exclusions in Article 2(2), Except for Negotiable Instruments

Article 2(2) of the ECL excludes several types of documents from coverage. The result is that the following types of documents must be in paper form to have legal validity: marriage and divorce; wills (Ross, 2005); deeds or registration of rights pertinent to real estate, and documents relating to sale, purchase or lease (in excess of ten years) of real estate; notarized documents; negotiable instruments; and other exclusions created in other laws. All of these exclusions should be eliminated, except for negotiable instruments. This would allow the electronic form to be used in all of the documents mentioned in the previous paragraph, other than negotiable instruments. This would firmly tell the world that the UAE sees virtually no limits to the utilization of the electronic form and would hasten the adoption of the electronic form by its citizens and residents. Only a few nations have been so bold in reducing exclusions (Azerbaijan, 2003), and so far none of them are in the Middle East.

b. Add: Consumer Protections in E-Commerce Contracts

The ECL fails to include consumer protections for E-commerce buyers. As a model, the UAE can look to Tunisia for an example of a nation with good consumer protections for E-commerce buyers. All of Tunisia's E-commerce consumer protections are commendable: (1) buyers have a "last chance" to review the order before it is entered into; (2) they have a 10-day window of opportunity to withdraw from the agreement after it has been made; (3) they have the right to a refund if the goods are late or if they do not conform to the specifications; and (4) the risk remaining on the seller during the 10-day trial period after the goods have been received (Tunisia, 2000).

c. Add: Several New Computer Crimes

The list of computer crimes needs to be expanded. The following computer crimes, with appropriate penalties, should be recognized: (a) Unauthorized Tampering with Computer Information; (b) Unauthorized Use of a Computer Service; (c) Unauthorized Interference in the Operation of a Computer; (d) Unauthorized Dissemination of Computer Access Codes or Passwords; and (e) Injection of a Virus into a Computer. The Singapore Computer Misuse Act can be used as a model (Singapore, 1993).

d. Add: Mandatory E-Government

Article 24 of the ECL contains E-government provisions, but they are permissive, not mandatory. The UAE is a wealthy nation with the monetary resources needed to purchase state-of-the-art computer information systems for their governmental departments. In order to reduce cost of government services and to make them 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. In Hong Kong, for example,

a substantial number of government services may now be accessed online, e.g., the scheduling of an interview for a visa or the scheduling of a wedding before a public official (Blythe, 2005).

e. Add: Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of the Kingdom of Nepal can be used as a model (Nepal, 2005).

f. Add: Explicit Long-Arm Jurisdiction

Because so many of the E-transactions will occur between UAE citizens and residents and parties outside the borders of UAE, it would be prudent for the UAE to formally state its claim of "long arm" jurisdiction against any party who is a resident or citizen of a foreign country, so long as that party has established "minimum contacts" with the UAE (Tonga, 2003). Minimum contacts will exist, for example, if a cyber-seller outside of the UAE makes a sale to a party living within UAE. In that situation, the ECL should be applicable to the foreign person or entity outside of UAE because that person or firm has had an effect upon UAE through the transmission of an electronic message that was received in UAE. The foreign party should not be allowed to evade the jurisdiction of the UAE courts merely because they are not physically present in the country. After all, E-commerce is an inherently international phenomenon.

7. Conclusions

The ECL's distinguishing attributes include: a convenient specification in its Preamble of all other statutes affected by it; a statement that any issues not addressed by the ECL are controlled by other bodies of law; a definition of a secure E-document; a provision that international contracting parties may agree to use a specific CSP, or to use a specific category of CSP's; provisions concerning E-contracts automatically made by pre-programmed computers; the mandatory deportation of a foreign citizen convicted of a computer crime; and the provision that invocation of a penalty for a computer crime will not prevent a more stringent penalty from being imposed pursuant to another law. Despite the admirable qualities of the ECL in its present form, there is room for improvement. Recommended refinements are to delete the exclusions from coverage (except for negotiable instruments) and to add the following: consumer protections, several new computer crimes, mandatory E-government, information technology courts, and explicit long-arm jurisdiction of those courts.

References

Azerbaijan, Republic of (2003). Electronic Document Law ("EDL"); http://unpan1.un.org. The EDL, for example, contains absolutely no exclusions from coverage; it states that electronic documents "can be used (applied) in *all activity spheres* where software and technical equipment could be applied to create, use, store, transmit and receive information." Id., art. 1(1). (Emphasis added.)

Blythe, Stephen E. (2007). Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region, Columbia Journal of East European Law 1:1, 44-75.

Blythe, Stephen E. (2006). The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute, Caribbean Law Review 16, 1.

Blythe, Stephen E. (2008). Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions, Transnational Law and Contemporary Problems 17:2, 361.

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

Blythe, Stephen 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.

Blythe, Stephen E. (2008). Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security, European Journal of Law and Economics 26:1, 75-103.

Blythe, Stephen E., The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries, Journal of Economics and Administrative Sciences 22:1, 103.

Blythe, Stephen E. (2005). Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's "Most Wired" City, North Carolina Journal of Law and Technology 7, 1.

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

Blythe, Stephen E. (2006). A Critique of India's Information Technology Act and Recommendations for Improvement, Syracuse Journal of International Law and Commerce 34, 1.

Blythe, Stephen E. (May, 2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security, Armenian Law Review; http://www.aua.am/aua/masters/law/pdf/esignaturelaw.pdf.

Blythe, Stephen E. (2006). Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures, Arab Law Quarterly 20, 317-344.

Blythe, Stephen E. (2006). Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal

Information Confidentiality and Controlling Computer Access, Journal of Internet Law 10, 20.

Blythe, Stephen 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, Stephen E. (November, 2008). E-Commerce and E-Signature Law of the United States of America, The Ukrainian Journal of Business Law; abstract: http://www.ujbl.info/; complete article: ftp://mail.yurpractika.com .

Blythe, Stephen E. (May, 2008). E-Signature Law and E-Commerce Law of the European Union and its Member States, The Ukrainian Journal of Business Law, 22-26; abstract: http://www.ujbl.info/.

Blythe, Stephen E. (2007). Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions, Information and Communications Technology Law 16:1, 47-71.

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

Blythe, Stephen E. (2008). On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law, Journal of High Technology Law, 8:1.

Blythe, Stephen E. (2006). Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce, Journal of Islamic State Practices in International Law 2:2, 5.
Blythe, Stephen E. (2006). Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality, Ohio Northern University Law Review 33, 525-562.

Blythe, Stephen E. (2007). Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions, The I.C.F.A.I. Journal of Cyber Law 6:4, 8-33.

Blythe, Stephen E. (2006). South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga, Journal of South Pacific Law 10:1.

Blythe, Stephen 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; http://www.hicbusiness.org/Proceedings_Bus.htm.

Blythe, Stephen E. (2006). Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World, Sri Lanka Journal of International Law 18.

Blythe, Stephen 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 Journal of International Law 28:3, 573-661.

European Union (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 On a Community Framework For Electronic Signatures—19 January 2000, OJ L OJ No L 13.

Fischer, Susanna Frederick (2001). California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation, Boston University Journal of Science and Technology Law 7, 234-37.

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; http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf. *See* (Blythe, 2008) supra.

Roland, Sarah 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 University Law Review 35, 638-45.

Ross, Chad Michael (2005). Comment, Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will. University of Memphis Law Review 35, 603. 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. Id.

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

Tonga, Kingdom of (2003). Computer Crimes Act (Act No. 14 of 2003); http://www.paclii.org/to/legis/num_act/cca2003185/. *See* (Blythe, 2006) supra.

Tunisia, Republic of (2000). Electronic Exchanges and Electronic Commerce Law; http://www.bakernet.com.org. *See* (Blythe, 2008) supra. Korea is one of the few nations that may offer better consumer protections than Tunisia. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act. *See* Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions ("CPA"), *Statutes of the Republic of Korea*, Vol. 13, pp. 481 to 485-30, originally enacted by Law No. 6687 (30 March 2002), and amended by Act Nos. 7315 and 7344 of 31 December 2004 and 27 January 2005, respectively. *See* (Blythe, 2006) supra.

United Arab Emirates ("UAE") (2006). Federal Law No. 1 of 30 January 2006 on Electronic Commerce and Transactions ("ECL");
http://www.tra.ae/pdf/legal_references/Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf.

United Nations Commission on International Trade Law, 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.

Utah, State of (1995). Utah Code Annotated 46-3-101 *et seq.*