International Business Research
www.ccsenet.org/ibr
Vol. 3, No. 1
January 2010

Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As A Sign of Hope for A Troubled Nation

Stephen E. Blythe
Professor of Law and Accounting
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

Abstract

Since it became independent in 1948, Burma has been plagued with a succession of military dictatorships. The present government refuses to recognize the election of Nobel Peace Laureate Aung San Suu Kyi, and keeps her under house arrest. Nevertheless, the legal foundation of Burma continues to develop, serving as a beacon towards a brighter day for the country. One example is the Electronic Transactions Law ("ETL") of 2004, a solid framework upon which E-commerce and E-government can be built in the future. The ETL recognizes the legal validity of electronic records, messages and signatures. The statute contains a third-generation E-signature law; all forms of electronic signatures are recognized, but a preference is given to the heightened security afforded by the digital signature. Commensurate with that preference, the ETL establishes a compulsory system of licensing of Certification Authorities ("CA"), prescribes detailed rules for them to follow, and assigns the Control Board to oversee their activities. The ETL contains a list of computer crimes, some of which are punishable by 15 years' imprisonment. Is the ETL up-to-date according to current trends in international E-commerce law? Not quite. Recommended amendments are to: (1)increase the potential liability of CA's; (2) recognize the legal validity of electronic wills; (3) add consumer protections; (4) claim "long arm" jurisdiction over foreign parties in E-commerce transactions; (5) compress the ETL's bureaucracy through consolidation of the Central Body and the Control Board; (6) provide for reciprocal recognition of foreign CA's and foreign certificates; and (7) establish informal Information Technology tribunals as a court-of-first-resort for E-commerce disputes.

Keywords: Burma, E-Commerce, Electronic, Signature, Transactions, Law

Objectives of the Article

The objectives of this article are to: (1) cover the recent history of Burma (CIA, 2009), its current state of economic development, and the nascent role of E-commerce as a part of that development; (2) explain the role of electronic signatures, public key infrastructure technology, and certification authorities; (3) describe the three generations of electronic signature law; (4) analyze Burma's Electronic Transactions Law ("ETL"); and (5) make recommendations for improvement of the ETL.

Introduction: Burma's Tragic Recent History

Burma was conquered by the British over a period of 62 years (1824-1886) and remained a British colony until achieving its independence in 1948. Since then, Burma has been a troubled nation, ruled by a succession of military strongmen with little concern for human rights and individual liberties. In the late 1980's, a pro-democracy political party—the National League for Democracy ("NLD")—grew in popularity. By the end of the decade, the NLD was on the threshold of power and attainment of democracy in Burma seemed to be a real possibility. The NLD's leader, Aung San Suu Kyi, was elected president of Burma in a landslide victory in 1990, despite the military opposition's interference in the campaign by placing her under house arrest before the election. Notwithstanding the election outcome, the military dictators refused to hand over power to her. Aung San Suu Kyi has courageously continued her efforts against the military *junta*. As a result, she has been kept under house arrest for fourteen of the past twenty years, including the present (CIA, 2009). For her "non-violent struggle for democracy and human rights" in Burma, she was awarded the Nobel Peace Prize in 1991 (Nobel Committee Presentation Speech, 1991; *see also* Nobel Committee's Biography of Aung San Suu Kyi, 1991) and is one of the author's "personal heroes." Her struggle remains difficult; the despotism of Burma's military dictatorship continues to this day (*see*, e.g., Sipress, 2005).

The traditional name of this nation is Burma. Since 1989, the military rulers of the country have touted "Myanmar" as the new name, but this has not been accepted by the United States and a number of other nations because it was never given approval by Burma's legislative body, which has been dissolved by the military dictatorship (CIA, 2009).

Burma's Economy and the Emergence of E-Commerce

Burma's Gross Domestic Product has been increasing during the past several years, mostly due to a rise in exports of oil and natural gas (State Department, 2009). Gross domestic product ("GDP") was recently estimated to be in excess of $55 billion. However, the development of the economy is hamstrung by extensive government controls and its inefficient economic policies. The government has imposed unrealistic official exchange rates that overvalue the nation's currency. Interest rates are distorted, fiscal deficits are the norm, official statistics relating to the GDP are unreliable, and there has been a failure to reconcile national accounts (CIA, 2009).

The plight of the ordinary people of Burma has continued to deteriorate during this decade. The annual per capita income of the population was recently estimated to be $1,200, but much of this income goes to the government and the wealthy; most of the citizens of Burma are forced to get by on an annual income of less than $200. The income of the people of Burma, already a pittance, has been further eroded by a decline in value of the currency; in 2008, the inflation rate was estimated to be 26%. Most Burmese are poorly educated with only eight or less years of education (CIA, 2009).

Apparently believing that free speech would undermine its control on power, the government strictly curtails access to the internet. Only about 40,000 people in Burma out of a population of 48.8 million use the internet (CIA, 2009; and State Department, 2009); Burma is 169th in the world on this statistic (CIA, 2009). Nevertheless, in order to stimulate the creation of reserves of foreign currency, the government has been encouraging the development to E-commerce sales by domestic firms to foreign parties. (E-commerce sales to domestic parties are limited by the small of people that have access to the web.) Accordingly, E-commerce is beginning to emerge, although there were only 108 internet hosts with websites in 2008 (CIA, 2009) E-government is also beginning to emerge, and the government has created a portal (Burma, Myanmar.com, 2009).

The Electronic Transactions Law ("ETL"), the major focus of this article, was created in 2004 to serve as the foundation for secure E-commerce transactions (Burma, ETL, 2004). Because of the potential ability of the internet, E-commerce and the ETL to improve the GDP of Burma and to open up the country to the world, these developments may be viewed as a sign of hope for a troubled nation.

Three Generations of Electronic Signature Law

Electronic Signatures

Contract law worldwide has traditionally required the parties to affix their signatures to a document (*see*, e.g., U.S. Uniform Commercial Code, 1998). 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," (Smedinghoff, 1999) 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" (European Union, 1999). An electronic signature may take a number of forms: a digital signature; biometric identifiers such as a voice pattern, facial recognition, a retinal scan, a digitized fingerprint or a digitized handwritten signature; a pin number; or merely a name typed at the end of an e-mail message (Tang, 1999).

Biometric identifiers have 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. The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers (Pun, 2002; *but see* Wright, 2001). Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card (Chung, 2003).

The digital signature is considered the most secure of all electronic signatures. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document (Hong Kong SAR, 2000). 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" (Smedinghoff, 1999). 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 (Poggi, 2000).

Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI" (Fischer, 2001). PKI consists of four steps:

1. The first step in utilizing this technology is to create a public-private key

pair; the private key will be kept in confidence by the sender, but the public key will be available online.

2. The second step is for the sender to digitally "sign" the message by creating

a unique digest of the message and encrypting it. A "hash value" is created

by applying a "hash function"—a standard mathematical function—to the

contents of the electronic document. The hash function is encrypted, or scrambled, by the signatory using his private key. The encrypted hash function is the "digital signature" for the document (Pun, 2002).

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

both to the recipient.

4. The fourth step is for the recipient to decrypt the digital signature by using

the sender's public key. If decryption is possible, the recipient knows the

message 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 (Zaremba, 2003).

The Critical Role of the Certification Authority

In order for PKI to realize its potential, it is crucial that the user be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If Smith and Jones are attempting to consummate an online transaction, Smith needs an independent confirmation that Jones' message is actually from Jones before Smith can have faith that Jones' public key actually belongs to Jones. It is possible that an imposter could have sent Jones his public key, contending that it belongs to Smith. Accordingly, a reliable third party—the Certification Authority ("CA")—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties (Hogan, 2000). The most important job of the CA is to issue certificates which confirm: the name and address of the CA that issued the certificate; the name, address and other attributes of the subscriber; the subscriber's public key; and the digital signature of the CA (Froomkin, 1996). Sufficient information will be contained in the certificate to connect a public key to the particular subscriber (Hogan, 2000).

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. 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). 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 (Roland, 2001).

The Second Generation of E-Signature Law: Technological Neutrality

Jurisdictions in the Second Generation 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. 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 the digital signature offers more security that other types of E-signatures (Blythe, 2009).

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 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). 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. The digital signature is given more respect under the Singapore statute, but it was not granted a monopoly as in the first generation. 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 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. 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; Burma is one of them.

Burma's Electronic Transactions Law

Objectives of the ETL

The Electronic Transactions Law (Burma, 2004: *hereinafter, "ETL"*) became effective on 30 April 2004 (ETL, Preamble). The purposes of the ETL are to: (1) facilitate the utilization of electronic transactions throughout Burma and thereby positively affect the development of the nation's human resources, economy, education and social services; (2) legally recognize electronic transactions having authenticity and integrity; and (3) improve domestic and international communication via transmission, reception and storage of data and messages in electronic form (ETL s 3). If any other laws of Burma conflict with the ETL, the ETL will prevail (ETL s 51).

Implementing Agencies of the ETL

The federal government department charged with responsibility for implementation of the ETL is the Ministry of Communications, Posts and Telegraphs ("Ministry") (ETL s 6(a)).

The Ministry appoints the members of the Central Body of Economic Transactions ("Central Body") and gives it financial support (ETL s 43). The Central Body is responsible for: (1) planning for application of information technology; (2) developing educational programs to teach information technology; (3) ensuring that the information technology adopted is commensurate, and will mesh, with information technologies of other nations that Burma may desire to interact with in the future; and (4) creation of an Electronic Transactions Control Board ("Control Board") to oversee the detailed, day-to-day aspects pursuant to the statutory purview (ETL ss 7, 9).

The Control Board's duties include: (1) licensing of Certification Authorities ("CA"), and consideration of recognition of a foreign CA for the purpose of doing business in Burma; (2) enforcement of the CA's qualification and experience requirements; (3) overseeing how the CA conducts its business, and inspecting the CA's records if necessary; (4) overseeing the relationship between the CA and its subscribers, and settling disputes between them; (5) regulation of the CA's computer information systems; (6) maintaining a publicly-accessible database (ordinarily, at its website) containing information regarding CA's; (7) investigation of any person or entity suspected of commission of computer crimes as defined in the ETL; and (8) periodically reporting its activities to the Central Body or to the Minister of Communications, Posts and Telegraphs (ETL s 10).

Both the Central Body and the Control Board are immune from civil or criminal liability so long as they have acted in good faith in the exercise of their duties (ETL s 49).

Exclusions

The trend in worldwide E-commerce law is that the typical list of exclusions (which prohibit utilization of electronic documents) is slowly being shortened. However, Burma does have a list of exclusions. Burma does not allow electronic documents to replace paper documents in: wills; negotiable instruments; trusts; powers of attorney; deeds and other title-related documents; instruments required by another law to be registered; and other matters to be determined by the Ministry (ETL s 5).

E-Government

Notwithstanding the list of exclusions, government agencies in Burma are encouraged to promote E-government policies as soon as possible. Accordingly, government agencies must recognize the validity of electronic documents in order to comply with: (1) document filing requirements of citizens; (2) document retention requirements of citizens and government; (3) issuance of licenses by government; and (4) making payments by citizens and government, and issuance of receipts (for payments) by citizens and government (ETL s 39). However, each government agency has the discretion to issue rules regarding format of the electronic document and security methods to be used (ETL s 40).

Legal Recognition of Electronic Documents and Signatures

The core of the ETL is contained in this sentence: *The legal validity of a record, message or signature will not be denied based on the mere fact that it happens to be in electronic form* (ETL s 48). However, the parties are allowed to make an agreement that only paper documents will be used (ETL s 20). Electronic records are admissible as evidence in a court of law if their integrity can be proven (ETL s 46). Furthermore, if a statute requires that documents must be retained, the electronic form will be permissible to satisfy this requirement (ETL s 39(a)). However, the party using the document may specify format and security requirements (ETL s 40).

Electronic Contract Rules

In the absence of a contrary agreement, a contractual offer and acceptance may be communicated in electronic form (ETL s 21).

Attribution

A receiver of an electronic message is entitled to presume that it has come from a specific sender, provided: (1) the sender sent the message, using the sender's ordinary procedure; (2) the sender's agent sent the message, using the sender's ordinary procedure; (3) the sender's computer information system (programmed by the sender or her agent) sent the message; or (4) the message was sent in accordance with a procedure previously agreed to by the sender and receiver (ETL ss 22-23).

Time of Dispatch and Receipt

An electronic message is deemed to have been sent when it enters a computer information system outside the control of the sender or her agent. The electronic message is considered to have been received when: (1) it enters the specific computer information system that the receiver requested it be sent to; however, if it enters another information system accessible to the receiver but not the one she specified, the applicable time is when the receiver retrieves it from the other system; or (2) if the receiver has not designated a specific computer information system for the message to be sent to, the applicable time is when the message enters any information system under the control of the receiver. These rules may be varied by agreement of the parties (ETL s 26).

Place of Dispatch and Receipt

The message will be assumed to have been sent or received from the respective business place of the sender or receiver. If the sender or receiver has more than one place of business, the principal place of business will apply. However, if the sender or receiver is a person and does not have a business place, the message is considered to have been sent from the person's "place of permanent residence." On the other hand, if the sender or receiver is a corporation, the place of transmission or receipt is its location of incorporation and legal establishment (ETL s 27).

Acknowledgement of Receipt

Before or at the time the message is sent, the parties may make an agreement as to how the receiver is to acknowledge receipt of the message. The acknowledgement may be in words, including words automatically generated by a computer information system; or it could be expressed through the receiver's conduct (ETL s 24). If the sender tells the receiver that the message is conditional on the sender's receipt of the acknowledgement, then the message is not considered to have been transmitted until the sender is in receipt of the confirmation. However, if the sender has requested an acknowledgement of receipt from the receiver (with no specified amount of time allowed for it to be made), but has failed to make the message conditional on the sender's receipt of the acknowledgement, then the sender is allowed to withdraw the message after the passage of a reasonable period of time. In the situation covered in the last sentence, but with a time limit placed upon the receiver for her to communicate the acknowledgment, the sender is

Regulation of Certification Authorities

The Certification Authority ("CA") plays a critical role in the public-key-infrastructure system. The CA's duty is to verify the authenticity of the electronic signature, i.e., that the signer is who she purports to be. The CA also has a duty to ensure the integrity of the electronic message that the electronic signature is affixed to, i.e., that it has not been altered since its creation (ETL s 10).

Licensing of CA's

The Ministry is authorized to make regulations relating to the duration of the license period, the initial license fee, and the fee for renewal of the license (ETL s 41). Any person or entity inside or outside of Burma may apply to the Control Board for a license (ETL s 12). Before the license is issued, the Control Board will require a prospective CA to: (1) prepare a Certification Practice Statement ("CPS"), which is a detailed list of the CA's policies, procedures and rules to be followed in the conduct of its business (ABA, 1995-96); (2) acquire a reliable and trustworthy computer information system which is suitable to the performance of its work;(3) establish a sound security system which will maintain the confidentiality of the subscribers' personal information; (4) show that it is capable of issuance of certificates containing all pertinent information; (5) show that it is capable of promptly disclosing to subscribers and relying third parties (using the CPS procedures) of any new facts which indicate that information in the certificate is inaccurate; and (6) comply with all other regulations prescribed by the Control Board (ETL ss 13-14).

Issuance, Suspension and
Revocation of Certificates by a CA

Any person may apply to a CA for issuance of a Certificate. One of the most common activities of a CA is to consider applications for Certificates, and to issue the Certificates if the applicants meet the qualifications (ETL s 16). It is important for the applicant to be entirely truthful in the information given to the CA. If issued, a Certificate must contain all pertinent information which a relying third party needs to verify the authenticity and integrity of the subscriber's electronic signature and the message it is attached to (ETL s 17(b)). The CA has a duty to either suspend or revoke a Certificate whenever the subscriber has not adhered to any condition stated in the Certificate, or has violated the ETL (ETL s 29).

Liability of Subscribers and CA's

The CA is immune from criminal or civil liability so long as it exercises its duties with reasonable care (ETL s 49). In the context of international E-commerce law, it is unusual to give the CA a virtual "free ride." Instead of the onus partially being placed on the CA, the ETL places it almost totally on the subscriber. The subscriber is obligated: (1) to ensure that all information in the Certificate is accurate; and (2) to maintain security over her private key and if it is lost or its security is compromised, to give prompt notice to the CA and to relying third parties (ETL s 17). If the subscriber fails to meet these obligations, she will be liable for consequential damages of relying third parties (ETL s 18).

Revocation or Suspension of the CA's License

If the conditions of the CA's license have not been complied with, or if the CA has violated the ETL, the Control Board may implement the following actions: (1) a penalty; (2) suspension of the CA's license for a period of time; or (3) revocation of the CA's license.

Computer Crimes

The ETL includes a number of penalties for computer crimes (ETL s 44). The computer crimes are enforceable by Burma's Police Force (ETL s 45).

Conviction of the following acts will result in imprisonment of 7 years (minimum) to 15 years, plus the possibility of a fine: (1) disclosure of state secrets; or (2) committing acts detrimental to national security, law and order, national solidarity, the national economy or the national culture (ETL s 33).

Conviction of these acts will result in a jail term of 5 years (maximum) and the possibility of a fine: (1) committing unauthorized acts of hacking, stealing, tampering, or modifying hardware or software used in a computer information system; (2) committing interception of computer messages without the permission of the sender and the receiver; (3) engaging in communication with another person, without authorization of said person, by using the person's "security number, password or electronic signature;" and (4) modifying the information contained in another's computer information system, and then disseminating that information to the detriment, embarrassment or harm of that person (ETL s 34).

A CA and its employees may be imprisoned for a period of 3 years (maximum), and may possibly be fined, for failing to abide by any prohibitions (e.g., the suspension or revocation of the CA's license, which would forbid the CA from operating its business either temporarily or permanently) listed in an order issued by the Control Board (ETL s 35).

Conviction of the following acts will be punished by a jail sentence of 1 year (maximum), plus the possibility of a fine: (1) Giving false information to a CA in an application for a Certificate, wrongfully pretending to be an agent of another in an application, or being an imposter when requesting the CA to suspend or revoke the Certificate; (2) failing to cooperate with the Central Body or the Control Board as they seek to carry out their duties pursuant to the ETL, or assaulting their integrity in an attempt to impugn their status; or (3) violation of a provision of the ETL (ETL ss 36-37).

Additionally, persons attempting or conspiring to commit the aforesaid acts, and those abetting the aforesaid acts, will be punished just as if they had been the principal party (ETL s 38). Finally, if a party defaults in the payment of a fine levied under the ETL, the Control Board may act against said party using the same procedures that would be applicable if the party was in “arrears of land revenue” (ETL s 42).

Recommendations for Improvement of Burma’s Electronic Transactions Law

Burma has made a commendable beginning toward attainment of a sound electronic transactions law. If Burma overcomes its political difficulties and is able to achieve a greater degree of economic growth, it will be able to take advantage of the opportunities that the ETL provides. Although the ETL is a significant accomplishment, it has not gone far enough. The following amendments should be considered.

Add: More Potential Liability for CA’s

As mentioned, it is unusual in international E-commerce law to find a situation of virtual immunity of CA’s. CA’s in Burma do not incur legal liability so long as they exercise reasonable care. This needs to be changed. Too much responsibility is placed upon the shoulders of the subscriber, and too little responsibility is placed upon the shoulders of the CA. Some of the burden of potential liability should be transferred from the subscriber to the CA. The computer law of the Republic of Vanuatu can be used as a model (Vanuatu, 2000).

Add: Recognition of Electronic Wills

The ETL excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature of the testator in order to be enforceable. This exclusion should be eliminated. 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 (Ross, 2005). Electronically-signed wills should be recognized.

Add: Long-Arm Jurisdiction against Foreign Parties

Because so many of the E-commerce transactions incurred by the residents of Burma will be with parties outside the borders of Burma, it would be prudent for the ETL to explicitly state its claim of “long arm” jurisdiction against any E-commerce party who is a resident or citizen of a foreign jurisdiction, so long as that party has established “minimum contacts” with Burma. The Kingdom of Tonga can be used as a model; that country explicitly states its claim of long-arm jurisdiction over foreign E-commerce parties (Tonga, 2003).

Minimum contacts will exist if a cyber-seller outside of the country makes a sale to a person in Burma. In that situation, the laws of Burma should be applicable to the foreign party because that party has had an effect upon the country through the transmission of an electronic message that was received in Burma. The foreign party should not be allowed to evade the jurisdiction of the Burmese courts merely because he is not physically present in the country. After all, E-commerce is an inherently international and multi-jurisdictional phenomenon.

Add: Reciprocal Recognition of Foreign CA’s and Their Issued Certificates

Most international E-commerce laws now provide for various forms of legal recognition of foreign CA’s and certificates issued in foreign countries. This is essential because E-commerce transactions often straddle international borders. Turkey’s Electronic Signature Law is a typical example and can be used as a model (Turkey, 2004).

Add: Consumer Protections for E-Commerce Buyers

Burma needs to enact a general consumer protection statute applicable to all internet consumers. The Republic of Tunisia can be used as a model for good consumer protections. The Tunisian E-commerce statute gives consumers: (1) a “last chance” to review an order before it is entered into; (2) a 10-day window of opportunity to withdraw from an agreement after it has been made; (3) a right to a refund if the goods are late or if they do not conform to specifications; and (4) no risk during the 10-day trial period after goods have been received. Tunisian E-consumers enjoy some of the best protections in the world (Tunisia, 2000).

Add: I.T. Courts for E-Commerce Disputes

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

Add: Consolidation of the Ministry's Bureaucratic Layers

Is it really necessary to have two bureaucratic layers of administration within the Ministry of Communications, Posts and Telegraphs? It's doubtful. The Central Body and the Control Board should be combined, and the consolidation should report directly to the Minister.

SUMMARY AND CONCLUSIONS

Since it became independent in 1948, Burma has been plagued with a succession of military dictatorships. The present government refuses to recognize the election of Nobel Peace Laureate Aung San Suu Kyi, and keeps her under house arrest. Nevertheless, the legal foundation of Burma continues to develop, serving as a beacon towards a brighter day for the country. One example is the Electronic Transactions Law ("ETL") of 2004, a solid framework upon which E-commerce and E-government can be built in the future. The ETL recognizes the legal validity of electronic records, messages and signatures. The statute contains a third-generation E-signature law; all forms of electronic signatures are recognized, but a preference is given to the heightened security afforded by the digital signature. Commensurate with that preference, the ETL establishes a compulsory system of licensing of Certification Authorities, prescribes detailed rules for them to follow, and assigns the Control Board to oversee their activities. The ETL contains a list of computer crimes, some of which are punishable by 15 years' imprisonment. Is the ETL up-to-date according to current trends in international E-commerce law? Not quite. Recommended amendments are to: (1)increase the potential legal liability of CA's; (2) recognize the legal validity of electronic wills; (3) add consumer protections; (4) claim "long arm" jurisdiction over foreign parties in E-commerce transactions; (5) compress the ETL's bureaucracy through consolidation of the Central Body and the Control Board; (6) provide for reciprocal recognition of foreign CA's and foreign certificates; and (7) establish Information Technology tribunals as a court-of-first-resort for E-commerce disputes.

A Final Comment

The author is optimistic that Burma will eventually overcome its political difficulties, achieve more recognition of human rights and re-join the world community. Burma is blessed with an abundance of natural resources and a hunger for democracy (as shown in the overwhelming vote for Aung San Suu Kyi in 1990). Most often, despotism does not prevail in the long run. Freedom can be expected to come to Burma. With it will come the Rule of Law, the lifting of controls over the internet, the necessary refinement of the Electronic Transactions Law, and the economic development of the country.

References

American Bar Association ("ABA"). (1995-96). Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce; http://www.abanet.org/ftp/pub/scitech/ds-ms.doc. The idea of a Certification Practice Statement ("CPS") originated with these Guidelines. The Guidelines define the CPS as "a statement of the practices which a certification authority employs in issuing the certificates." Id. at s 1.8.

Berman, Andrew B. (2001). Note, "International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 Syracuse *Journal of International Law and Commerce* 125.

Blythe, Stephen E. (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. (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. (2007). 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. (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. (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. (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. (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. (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. (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). 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. (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.

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

Blythe, Stephen E. (May 19-23, 2009). "The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control," Proceedings of the Tenth Annual Conference of the International Academy of African Business and Development, Kampala, Uganda.

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

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, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12.

Fischer, Susanna Frederick. (2001). California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation, Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, *Boston University Journal of Science and Technology Law* 7, 229-237.

Froomkin, A. Michael. (1996). The Essential Role of Trusted Third Parties in Electronic Commerce, *Oregon Law Review*, 75, 49 and 58.

Hallerman, David. (June 1, 1999). Will Banks Become E-commerce Authorities?, Bank Technology News, 12.

Hogan, Tara C. (2000). Notes and Comments—Technology, Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?, North Carolina Banking Institute 4, 417 and 424-25.

Hong Kong Special Autonomous Region. (2000). Electronic Transactions Ordinance, Ord. No. 1 of 2000, s 2. 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." Id.

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* Blythe, Stephen E. (2008).

Nobel Committee. (1991). AUNG SAN SUU KYI—BIOGRAPHY;

http://nobelprize.org/peace/laureates/1991/kyi-bio.html.

Nobel Committee. (1991). PRESENTATION SPEECH: THE NOBEL PEACE PRIZE 1991; http://nobelprize.org/peace/laureates/1991/index.html.

Poggi, Christopher T. (2000). Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation, *Virginia Journal of International Law* 41, 224-251.

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

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

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

Sipress, Alan. (29 December 2005). Burma Raises the Drawbridge: Rangoon Has Removed Itself to the Hinterland in a Move That's Shocked Everybody," The Standard, Hong Kong, p. A27. Citizens of Burman were shocked in 2005 by a rash decision of the nation's dictator—military strongman General Than Shwe—to move the capital from Rangoon to Pyinmana, a desolate location 322 kilometers north of Rangoon. Pyinmana is located in a sparsely-populated, malaria-infested region of the country, and had very little housing to accommodate the civil servants who were forced to relocate there. Foreign nations having relations with Burma were expected to undergo the expense of construction of new embassies. Id.

Smedinghoff, Thomas J. (1999). Electronic Contracts: An Overview of Law and Legislation, PLI/P 564, 125-162.

Stern, Jonathan E. (2001). Note, Federal Legislation: The Electronic Signatures in Global and National Commerce Act, *Berkeley Technology Law Journal* 16, 391-395.

Tang, David K.Y. Electronic Commerce: American and International Proposals for Legal Structures, a book chapter in Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries 333 (Christopher McCrudden, Editor).

Tonga, Kingdom of, Computer Crimes Act, 2003. *See* Blythe, Stephen E. (2006).

Tunisia, Republic of. (2000). Electronic Exchanges and Electronic Commerce Law; http://www.bakernet.com.org.

Turkey, Republic of. Electronic Signature Law, 2004, art. 14.

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

United Nations. (1998). 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.

United States of America, Central Intelligence Agency ("CIA"), "Burma," THE WORLD FACTBOOK, 2009, pp. 1, 2, 5, 7, 8, 12, 13; https://www.cia.gov/library/publications/the-world-factbook/geos/bm.html .

United States of America, U.S. Department of State ("State Department"), Bureau of East Asian and Pacific Affairs, BACKGROUND NOTE: BURMA (July, 2009), pp. 1-2; http://www.state.gov/r/pa/ei/bgn/35910.htm . Other natural resources which are abundant in Myanmar include timber, tin, antimony, coal, limestone, tungsten, zinc and precious stones. Id.

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

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

Vanuatu, Republic of. (2000). Electronic Transactions Act, s 23(1)(a)-(c). In Vanuatu, CA's are liable to relying third parties for: (1) the truthfulness of all information contained in the Certificate as of the issue date, unless a contrary statement appears on the Certificate; (2) its assurance that the subscriber held the private key (the signature creation device) on the date of issuance, which corresponds to the public key (signature verification device) listed or identified in the Certificate; and (3) if the CA generates both the private key and the public key, assurance that the two keys function together in an acceptable manner. *See* Blythe, Stephen E. (2006).

Wright, Benjamin. (2001). Symposium: Cyber Rights, Protection, and Markets: Article, Eggs in Baskets: Distributing the Risks of Electronic Signatures, West Los Angeles Law Review, 32, 215-226 (2001). Wright, an expert in computer law and technology, is a notable exception. He contends that biometrics is a more preferable authentication method in the case of the general public, although he concedes that digital signatures using PKI are preferable for complex financial deals carried out by sophisticated persons. In PKI, control of the person's "private key" becomes all-important. The person must protect the private key; all of the "eggs" are placed in that one basket, and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public would be sharing the risk with other parties involved in the transaction, and the need to protect the "private key" is not so compelling. Id.

Zaremba, Jochen. (2003). International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers, Connecticut Journal of International Law 18, 479- 512.