ARMENIA'S ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE LAW: PROMOTION OF GROWTH IN E-COMMERCE VIA GREATER CYBER-SECURITY

Stephen E. Blythe[1]

Abstract

Armenia's Electronic Document and Electronic Signature Law ("EDL") was enacted in 2004 and provides for legal recognition of electronic signatures, but the only type of electronic signature accepted is the digital signature; hence, the statute requires the utilization of cryptographic methods in order to achieve a heightened degree of reliability and security. The EDL regulates Certification Centers, often referred to as certification authorities ("CA") in other jurisdictions. A CA is not required to achieve accredited status, but it may voluntarily do so if it is able to comply with financial, technical expertise and other requirements. The principal duties of CA's are to issue certificates to successful applicants and to confirm the authenticity and integrity of electronic signatures to relying third parties. Before issuance of the certificate, the CA must confirm the identity of the applicant and ensure that all information received in the application is accurate. The CA is responsible for maintaining the security of all information that it receives from the applicant. When a certificate is issued, the subscriber will be given the private key which will enable him to "sign" electronic documents. CA's must maintain a publicly-accessible repository of certificates and the public keys which can be used to decrypt the subscriber's message. A CA may incur legal liability for publishing a certificate with inaccurate information or for failing to suspend or terminate the validity of the certificate if there is a possibility of inaccurate information or fraudulent activity. The EDL is a good first-step, but it needs to be amended to include: recognition of all types of E-signatures, including biometrics, while continuing to give the digital signature most-favored-status; rules relating to evidentiary admissibility of E-documents and E-signatures; E-contract rules, including consumer protections and carriage contracts; a comprehensive list of computer crimes; information technology courts; and cybersuites.

---

[1] Professor of Law and Accounting, New York Institute of Technology, CERT Technology Park, Abu Dhabi, United Arab Emirates. Ph.D. Candidate (Int'l E-Commerce Law), The University of Hong Kong (China); Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law) University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. He practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance-defense litigation) in Oklahoma City, and was a management consultant for the city of Haikou, China. Additionally, he has taught law, accounting, management, economics and international business at fifteen universities located in the United States, Africa and the Middle East.

ARMENIA'S ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE LAW: PROMOTION OF GROWTH IN E-COMMERCE VIA GREATER CYBER-SECURITY

OBJECTIVES OF THE ARTICLE

The objectives of this article are to: (1) introduce the reader to Armenia's economy and internet usage; (2) explain the role of electronic signatures, cryptology, public key infrastructure, and certification authorities; (3) cover the three generations of electronic signature law; (4) analyze Armenia's Electronic Document and Electronic Signature Law ("EDL"); and (5) make recommendations for improvement of that statute.

ARMENIA'S ECONOMY AND THE INTERNET

As a part of the Soviet Union from 1920 to 1991, Armenia had developed its industrial sector and supplied machine tools and textiles to other Soviet republics in exchange for raw materials and energy.[2] Armenia became an independent republic following the collapse of the Soviet Union in 1991.[3] By 1994, the new Armenian government had implemented economic reforms including privatization, price reforms and sound fiscal policies.[4] The new economic policies included a change to small-scale farms instead of the large collective farms of the Soviet era.[5] The economic reforms were successful, resulting in a reduction of poverty, decrease in inflation, and stabilization of the currency.[6] Armenia is blessed with mineral deposits (e.g., copper, gold and bauxite), and its primary exports are pig iron, unwrought copper and other nonferrous metals.[7] In recent years, the average rate of economic growth has been in excess of 13%, a very impressive statistic.[8] Armenia's gross domestic product ("GDP") was estimated to be US $16.83 billion in 2007.

Despite the high economic growth rate, Armenia did have a moderately high rate of unemployment in the same year, estimated at 7.1%.[9] Additionally, 26.5% of Armenians

---

[2] U.S. Central Intelligence Agency ("CIA"), THE WORLD FACTBOOK, "Armenia," 20 March 2008, pp. 8-9; http://www.cia.gov/library/publications/the-world-factbook/print/am.html .
[3] Id. at 2.
[4] Id. at 8.
[5] Id. at 9.
[6] Id. at 8.
[7] Id. at 9.
[8] Id. at 8.
[9] Id. at 10.

are impoverished.[10] To combat the unemployment and poverty problems, Armenia needs to pursue further economic reforms in order to become more competitive in the global economy. Unfortunately, Armenia's economy is disadvantaged by the fact that she is economically isolated from two of her nearest neighbors—Azerbaijan and Turkey.[11]

Armenia has more than 8,000 internet hosts and 9 internet service providers.[12] Although less than 200,000 of the 3 million Armenians use the internet, the percentage of computer-literate Armenians continues to grow.[13] Because of this, the number of E-commerce and E-government transactions are expected to increase in the future. Furthermore, the Electronic Document and Electronic Signature Act[14]--the focal point of this article--has created a sound legal infrastructure and heightened security requirements for electronic transactions. These legal developments should further promote the growth of E-commerce and E-government in Armenia.

ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[15] 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,"[16] 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."[17] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[18]

---

[10] Id. at 10.
[11] Id. at 9.
[12] Id. at 13.
[13] Id. at 13-14.
[14] EDL, Note 84 infra.
[15] *See*, e.g., the U.S. UNIFORM COMMERCIAL CODE ss 2-201 and 2-209 (1998).
[16] Thomas J. Smedinghoff, "Electronic Contracts: An Overview of Law and Legislation," 564 PLI/P at 125, 162 (1999).
[17] 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. Under Armenian law, an electronic document is defined as "information or message presented in electronic version." EDL, note 84 infra, art. 2. The EDL notes that an electronic document has two forms: an "internal," or digital form, recorded on an electronic carrier (e.g., magnetic disk, tape, laser disk, or semi-conductor); and an "external" form reproduced on a tangible thing (e.g., on paper or a CRT screen) and "visually accessible and readily perceptible." Id., art. 3.
[18] 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).

A well-known U.S. consumer group has stated, "Given the current state of authentication technology, it's much easier to forge or steal an e-signature than a written one."[19] This statement seems to assume that all E-signatures offer an equal degree of security. However, such an assumption would be erroneous; some electronic signatures offer more security than others. It is prudent for E-commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

Online Contracts:
Four Levels of Security

When entering into a contract online, four degrees of security are possible.

a. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[20]

b. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased.[21]

c. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief. Examples include: a voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, a digital reproduction of a fingerprint,[22] or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison with a person purporting to have the same identity.[23] For example, if a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter.[24]

---

[19] Michael Dessent, "Browse-Wraps, Click-Wraps and Cyberlaw: Our Shrinking (Wrap) World," 25 THOMAS JEFFERSON LAW REVIEW 1, 4 (Fall, 2002).

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

[21] Id.

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

[23] Note 20 supra at 395-96; and "The Legality of Electronic Signatures Using Cyber-Sign is Well Established," CYBER-SIGN, at http://www.cybersign.com/news_news.htm.

[24] Id.

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;"[25] 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.[26] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[27] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[28]

d. The digital signature is considered the fourth level because it is more complex than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document.[29] 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."[30] 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.[31]

---

[25] 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 (2002).

[26] Id. at 257.

[27] Id. However, one of the experts in computer law and technology—Benjamin Wright—is a notable exception. Wright contends that biometrics is a more preferable authentication method in the case of the general public, although he concedes that digital signatures using PKI (covered infra) are preferable for complex financial deals carried out by sophisticated persons. In PKI, control of the person's "private key" becomes all-important. The person must protect the private key; all of the "eggs" are placed in that one basket, and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public would be sharing the risk with other parties involved in the transaction, and the need to protect the "private key" is not so compelling. See Benjamin Wright, "Symposium: Cyber Rights, Protection, and Markets: Article, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures,'" 32 WEST LOS ANGELES LAW REVIEW 215, 225-26 (2001).

[28] Note 22 supra.

[29] 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.

[30] Note 16 supra at 146.

[31] 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).

<u>Digital Signature Technology:</u>
<u>Public Key Infrastructure</u>

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI."[32] PKI consists of four steps:

a. The first step in utilizing this technology is to create a public-private key pair; the private key[33] will be kept in confidence by the sender,[34] but the public key[35] will be available online.[36]

b. The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it. A "hash value" is created by applying a "hash function"—a standard mathematical function—to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Whereupon, the hash function is encrypted, or scrambled, by the signatory using his private key. Asymmetric encryption provides one of the highest—if not *the* highest—degrees of security in electronic transactions. The encrypted hash function is the "digital signature" for the document.[37]

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

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

---

[32] 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 (Summer, 2001).

[33] Under Armenian law, the private key is referred to as the "electronic signature-creation device" and is defined as "configured software or hardware used to create electronic signature by signature-creation data." EDL, Note 84 infra, art. 2. Signature-creation data are described as "unique sequence of symbols, which is used by the signatory to create an electronic signature." Id.

[34] American Bar Association ("ABA"), PKI ASSESSMENT GUIDELINES, V 0.30 at 301 (Public Draft for Comment No. 25, 2001); http://www.abanet.org/scitech/ec/isc/pagv30.pdf. Under Armenian law, the sender is the person signing the electronic document; he is referred to as a "signatory" and is defined to be "an individual (or the person he represents) in whose name the certificate of electronic signature has been given." EDL, Note 84 infra, art. 2.

[35] Under Armenian law, the public key is referred to as a "signature-verification device" and is defined as "configured hardware or software used to verify the authenticity of electronic signature by signature-verification data." EDL, Note 84 infra, art. 2. Signature-verification data (often referred to as simply "verification data") are defined as "unique sequence of symbols, which is used to verify an electronic signature." Id. Electronic signature authenticity refers to a "positive result of use of signature-verification data and devices, which identifies the signatory." Id.

[36] Note 34 supra at 305.

[37] Note 25 supra at 249.

the decrypted message digest.[38] If they match, the recipient knows the message has not been altered.[39]

Advantages of the Digital Signature

Unlike biometric and other forms of electronic signatures, the digital signature will "freeze" the contents of the document at the time of its creation. Any alterations to the document's contents will result in a different hash value. Furthermore, the encryption of the hash value with the signatory's private key "links uniquely the digital signature to the signatory, i.e., the owner of the private key." [40] Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific." [41]

The digital signature is the only form of electronic signature which satisfies all three of the UNCITRAL security evaluation factors, i.e., that an electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud. [42] Authorization is achieved because the digital signature will accompany the document, which allows for confirmation of the identity of the signatory. Approval is attained via computation of the hash value of the electronic document, which freezes the contents of the document at the time of its creation, and allows for detection of any subsequent alterations. Finally, there is protection against fraud because it is extremely unlikely—virtually impossible—for anyone to determine a signatory's private key with only the public key as a starting point.[43]

Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. Firstly, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common to most other forms of electronic signatures. The password or the PIN face similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized.[44]

---

[38] American Bar Association, Section of Science & Technology, Information Security Committee, Electronic Commerce & Information Technology Division, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (ABA Net, 1995 and 1996) p. 9; http://www.abanet.org/ftp/pub/scitech/ds-ms.doc .
[39] Jochen Zaremba, "International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers," 18 CONNECTICUT JOURNAL OF INTERNATIONAL LAW 479, 512 (2003).
[40] Note 25 supra at 250.
[41] Id.
[42] Note 25 supra at 243.
[43] Note 25 supra at 252.
[44] Note 25 supra at 253.

The other disadvantage of the digital signature pertains to the certificate,[45] which must be issued by a Certification Authority ("CA").[46] Obtaining the certificate and having to interact with the CA is somewhat inconvenient and costly for the user, but over time this disadvantage should be alleviated as digital signatures become more popular, easier to use, and cheaper.[47] Because the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

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 A (the sender) and B (the receiver) are attempting to consummate an online transaction, B needs an independent confirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that an imposter could have sent B the public key, contending that it belongs to A when in fact it does not. Accordingly, a reliable third party—the Certification Authority—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[48]

The most important job of the CA is to issue certificates which confirm basic facts about the subscriber, the subject of the digital certificate. The certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties: 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.[49] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[50]

In making an application to a CA for a certificate, the prospective subscriber must provide some sort of photo I.D., e.g., a passport or a driver's license. If the application is approved and the certificate is issued, the CA will issue a private key to its new subscriber which corresponds to the public key. This is done, however, without disclosing the specifics of the private key.[51] The steps in this application procedure vary

---

[45] Under Armenian law, the "electronic signature certificate" is defined as "a document (either paper-based, or electronic or on another carrier), which links signature-verification data to a signatory and confirms the identity of that person and serves as electronic signature-verification device." EDL, note 84 infra, art. 2.

[46] Under Armenian law, the CA is referred to as a "certification center." EDL, note 84 infra, art. 2. Armenia is the only jurisdiction this researcher has seen which uses that term. CA, the term used in this article, is used in most of the world's jurisdictions with the exception of the European Union, which uses "certification service provider."

[47] Note 25 supra at 253.

[48] Tara C. Hogan, Notes and Comments—Technology, "Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?," 4 NORTH CAROLINA BANKING INSTITUTE 417, 424-25 (2000).

[49] A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 OREGON LAW REVIEW 49, 58 (1996).

[50] Note 48 supra at 425-426.

[51] Note 16 supra at 149.

somewhat from CA to CA, according to the type of certificate being offered by the CA. Ordinarily, however, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued.[52]

In order to indicate the authenticity of the digital certificate, the CA will sign it with his digital signature. Typically, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties who have need of communication with the subscriber. Additionally, the online repository contains information pertaining to digital certificates which have been revoked or suspended by the CA due to lost or expired private keys. This is an important positive aspect of PKI technology: the general public has access to the status of digital signatures, and relying third parties are kept informed, allowing them to judge whether they should place reliance on communications signed with a certain private key.[53]

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber.[54] Nations around the world have arrived at different conclusions regarding this apportionment. The problem is compounded if each CA is required to modify its practices every time it issues a certificate pertaining to a transaction affecting another jurisdiction which happens to have dissimilar digital signature laws.[55]

A certificate is only as reputable as the CA that issues it. If the CA is unreliable and untrustworthy, the certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate.[56]

THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

The First Wave: Technological Exclusivity

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[57] In the Utah statute, digital signatures were given legal

---

[52] Note 16 supra at 150.
[53] Note 48 supra at 426-27.
[54] Michael J. Osty and Michael J. Pulcanio, "The Liability of Certification Authorities to Relying Third Parties," 17 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW 961 (1999).
[55] *See* Andrew B. Berman, Note, "International Divergence: The 'Keys' To Signing on the Digital Line— The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 125, 143-44 (2001); and Alana Maurushat, 35:3 HONG KONG LAW JOURNAL 569 (2005), arguing that multi-lateral recognition of CA's among China, Hong Kong and Singapore should only occur after their PKI legislation has been harmonized and each of them provides sufficient privacy protections for personal data.
[56] David Hallerman, "Will Banks Become E-commerce Authorities?," 12 BANK TECHNOLOGY NEWS, June 1, 1999.
[57] UTAH CODE ANNOTATED 46-3-101 *et seq.* (1999).

recognition, but other types of electronic signatures were not.[58] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature include Armenia, Germany, India,[59] Italy, Malaysia, Nepal[60] and Russia.[61]

 Unfortunately, these jurisdictions' choice of "technological-exclusivity" 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.[62]

   The Second Wave: Technological Neutrality

Jurisdictions in the Second Wave overcompensated. They did the complete reversal of the First Wave and did not include any technological restrictions whatsoever in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the others. In other words, they are "technologically neutral." Permissive jurisdictions provide legal recognition of many types of electronic signatures and do not grant a monopoly to any one of them. Examples of permissive jurisdictions include the majority of states in the United States, the United Kingdom,[63] Australia and New Zealand.[64]

---

[58] Id.

[59] 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); Available at Lexis-Nexis:
http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=140728&docNo=3.

[60] Stephen E. Blythe, "On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law," forthcoming in 8:2 JOURNAL OF HIGH TECHNOLOGY LAW ___(2008).

[61] Note 32 supra at 234-37.

[62] 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).

[63] For concise coverage of American and British law, *see* Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security," 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005). Available at
http://law.richmond.edu/jolt/v11i2/article6.pdf and at Lexis-Nexis:
http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=156342&docNo=7 .

[64] Note 32 supra at 234-37.

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.

The Third Wave: A Hybrid

Singapore was in the vanguard of the Third Wave. In 1998, this country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce.[65] 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. Singapore did not want to become "hamstrung" by tying itself to a one form of technology. The Singapore legislators realized that technology is continually evolving and that it would be unwise to require one form of technology to the exclusion of others. The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[66]

The moderate, hybrid position taken by Singapore has become the progressive trend in international electronic signature law and has been adopted in many jurisdictions,

---

[65] United Nations Commission on International Trade Law ("UNCITRAL"), MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT (hereinafter "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/english/texts/electcom/ml-ecomm.htm. *See* Stephen E. Blythe, Note 63 supra.
[66] Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88), 10 July 1998; http://agcvldb4.agc.gov.sg/. Although granting legal recognition to most types of electronic signatures, the Singapore statute implicitly makes a strong suggestion to users—in two ways—that they should use the digital signature because it is more reliable and more secure than the other types of electronic signatures: (1) digital signatures are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carry a legal presumption of reliability and security—these presumptions are not given to other forms of electronic signatures; and (2) although all forms of electronic signatures are allowed to be used in Singapore, its electronic signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the of authenticity and integrity of electronic messages affixed to electronic signatures. Id. *See* Stephen E. Blythe, "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33:2 OHIO NORTHERN UNIVERSITY LAW REVIEW 525-562 (2007); Available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=140724&docNo=1 .

including these: Azerbaijan,[67] Barbados,[68] Bermuda,[69] China,[70] Dubai,[71] European Union,[72] Finland,[73] Hong Kong,[74] Hungary,[75] Iran,[76] Japan,[77] Lithuania,[78] Pakistan,[79] South Korea,[80] Taiwan,[81] Tunisia[82] and Vanuatu.[83]

---

[67] 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).

[68] Stephen E. Blythe, "The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute," 16 CARIBBEAN LAW REVIEW ___ (2007).

[69] Note 32 supra at 234-37.

[70] Stephen E. Blythe, "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce," 7 CHICAGO-KENT JOURNAL OF INTELLECTUAL PROPERTY 1 (2007). Available at http://jip.kentlaw.edu/currentissue.asp
and at Lexis-Nexis:
http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=221052&docNo=2.

[71] 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," 23:1 JOURNAL OF ECONOMICS AND ADMINISTRATIVE SCIENCES (2007). Available at: http://jeas.cbe.uaeu.ac.ae/ .

[72] Note 17 supra. *See* Stephen E. Blythe, Note 63 supra.

[73] Stephen E. Blythe, "Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services," 31:1 HAMLINE LAW REVIEW (2007).

[74] Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. *See* Stephen E. Blythe, "Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's 'Most Wired' City," 7 NORTH CAROLINA JOURNAL OF LAW AND TECHNOLOGY 1 (2005). Available at http://www.jolt.unc.edu/currentissue.htm and at Lexis-Nexis:
http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=241400&docNo=5 .

[75] Stephen E. Blythe,"Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions," 15 INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 47 (2007); http://www.tandf.co.uk/journals/journal.asp?issn=1360-0834&linktype=5 .

[76] 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).

[77] Stephen E. Blythe, "Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access," JOURNAL OF INTERNET LAW (July, 2006), a publication of Aspen Publishers, Inc., New York, NY USA. Available at:
http://www.accessmylibrary.com/coms2/summary_0286-17306641_ITM.

[78] Stephen E. Blythe, "Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions," 8 BARRY LAW REVIEW 23 (2007). Available at Lexis-Nexis:
http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T32295 58475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22 _T3229558479&treeMax=true&treeWidth=0&csi=254558&docNo=6.

[79] 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 __ (2006). Available at: http://electronicpublications.org/catalogue.php?id=46.

[80] 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 (2006).

[81] 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

ARMENIA'S ELECTRONIC DOCUMENT
AND ELECTRONIC SIGNATURE LAW

Armenia's Electronic Document and Electronic Signature Law (hereinafter "EDL") was enacted in 2004.[84] The purpose of the EDL is to provide a legal framework for the use of E-documents and E-signatures.[85]

E-Documents

If a statute requires the production of an original paper document in order to incur a legal right, that requirement will be deemed to have been met by production of an authenticated E-document, with supporting evidence that the document has not been altered since its creation (other than electronic notations necessary for storage of the document).[86] If paper copies are made from an E-document to be filed for an official purpose, the copies should be certified using the procedure specified by the EDL and should indicate on their face they have been copied from an E-document.[87] If a statute mandates that paper documents are to be stored, that mandate will be deemed to have been met if a copy of the paper document is stored as an E-document; however, the document must not have been altered and must be capable of being reproduced in its original form. The verification data used to confirm the authenticity of the E-document must also be stored properly along with the E-document.[88]

E-Signatures

The EDL is a first-generation E-signature law; the only type of E-signature recognized is the digital signature. This is obvious from the EDL's definition of an E-signature: "obtained signature-creation data and a cryptographic data modification of the given electronic document presented in a unique sequence of symbols in electronic form, which is attached or logically associated with an electronic document and which is used to

---

HAWAII INTERNATIONAL CONFERENCE ON BUSINESS, Honolulu, Hawaii U.S.A., May 25-28, 2006. Available at: http://www.hicbusiness.org/Proceedings_Bus.htm.

[82] Stephen E. Blythe, "Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures," 20 ARAB LAW JOURNAL 240-67 (2006). Available at: http://www.ingentaconnect.com/content/brill/alq.

[83] 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). Available at: http://www.paclii.org/journals/fJSPL/vol10/ .

[84] Republic of Armenia, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE ("EDL"), 2004; http://www.gipi.am/?i=223 .

[85] EDL art. 1(1). However, the EDL is inapplicable to the emerging area of "transformed electronic and other analogues of handwritten signature and documents signed by those analogues." In other words, the EDL is inapplicable to a digitized image of a handwritten signature which can be attached to an E-document. EDL art. 1(2).

[86] EDL art. 5. The format of the E-document should be "understandable and accessible for the person's perception not having technical education." Id.

[87] EDL art. 6.

[88] EDL art. 7.

identify the signatory, as well as to protect the electronic document from forgery and distortion."[89] This is an exclusive definition and is not an indication of technological open-mindedness. Other E-signatures, such as biometrics, would not fulfill the requirements of that definition and would be unacceptable.

If a statute requires the presence of a handwritten signature in order to incur a legal right, that requirement is deemed to have been met if a secure, authenticated E-signature has been attached to an E-document; the digital signature is the only type that is acceptable.[90]

<div align="center">Certification Authorities</div>

The EDL distinguishes an ordinary CA from an accredited CA. An ordinary CA is defined as an "organization that issues certificates or provides other services related to electronic signatures."[91] An ordinary, unaccredited CA does not need a license to operate. An accredited CA is one which has obtained accreditation "in accordance with the rules and procedures defined by the Armenian legislation."[92] CA's have the following duties: contract with subscribers to issue a certificate; issue a certificate after confirmation of identity of subscriber and explaining relevant information to the subscriber, to include restrictions stated in the certificate; issue the private key to subscriber, and do not keep a record of the private key without the permission of subscriber; keep records of issued certificates and the current status of each; publish the public key at its website; and ensure security of E-signatures and authenticate them.[93]

The procedure to be used in creation of an E-signature will be determined by the "manufacturer of the electronic signature creation device."[94] E-signature verification data may be created by either the CA or the subscriber using hardware or software. The verification data and the certificate will be distributed by the subscriber to the person he is communicating with, or by a CA upon request by an interested party.[95] The certificate issued to the subscriber by the CA must contain the following information: registration number; name and address of the subscriber and CA; public key (verification data); period of validity; restrictions on purpose and limitation on amount of financial transaction; and limitations of CA's liability.[96]

---

[89] EDL art. 2.

[90] EDL art. 4. However, governmental agencies are not mandated to accept an E-document signed with an E-signature if they do not have the technical capability necessary for acceptance. Id.

[91] EDL art. 2. Armenia refers to a CA as a "Certification Center." CA is used in this article because this term is in much greater use internationally. *See* Note 46 supra.

[92] EDL art. 2. The government maintains a registry of accredited CA's and periodically inspects them to ensure they are in compliance with the EDL and its implementing regulations. EDL art. 15. Accredited CA's must take extra precautions to ensure the security and integrity of their technical systems, and must provide a higher degree of service to the subscriber and relying third parties. EDL art. 16.

[93] EDL art. 12.

[94] EDL art. 8.

[95] EDL art. 9.

[96] EDL art. 13.

If a CA goes out of business either voluntarily or pursuant to a court order, the CA should get the permission of its subscribers to transfer its responsibilities to another CA.[97]

If the EDL is in conflict with an international treaty entered into by the government of Armenia, the international treaty will prevail.[98] Accordingly, it may be assumed that foreign CA's and certificates issued by foreign CA's will have legal validity in Armenia if an international treaty exists between Armenia and the foreign nation.

RECOMMENDATIONS FOR IMPROVEMENT OF THE EDL

Jump from the First Wave
to the More Progressive Third Wave

The third generation of E-signature laws is the current trend and appears to be the compromise position that the nations of the world will coalesce around: all E-signatures will be recognized and accepted, but the digital signature is placed on a pedestal and given special status and privileges. Armenia's EDL should be modified to accept this third generation position.

Add E-Contract Rules

Many nations of the world have adopted rules for E-contracts. Armenia also needs them. Specific rules should be enacted pertinent to: attribution of an E-message; acknowledgement of receipt of an E-message; assumed time and place of transmission and receipt of an E-message; and other essential issues. Any number of E-commerce laws could be used as a model; Barbados is but one example.[99]

Special Rules for
Carriage Contracts

Because of the special requirements pertinent to contracts for the delivery of goods, or "carriage" contracts, some jurisdictions have adopted special rules for them. In consideration of this possibility, Armenia can look to the E-commerce law of Colombia[100] and Canada[101] for examples.

---

[97] EDL art. 17.
[98] EDL art. 10.
[99] Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B, 8 March 2001, s 14-16; http://www.barbadosbusiness.gov.bb/miib/Legislation/Acts/investment_acts.cfm . *See* Stephen E. Blythe, Note 68 supra.
[100] Colombia's statute contains rules regarding these and other aspects of a carriage contract: (1) detailed description of the goods; (2) issuance of receipt; (3) confirmation of shipment; (4) notification of terms of the contract; (5) instructions to be conveyed to the transporter; (6) request of delivery of the goods; (7) authorization to deliver the goods; (7) buyer's notification of loss or damage of goods during transit; (8) seller's promise to deliver the goods to buyer or her agent; and (9) acquisition, waiver or transfer of rights in the agreement. In Colombia, E-documents may be used in the creation or implementation of carriage

Consumer Protections in E-Contracts

Consumer protections for E-commerce buyers are needed. As a model, Armenia can look to Tunisia's computer law for good consumer protections:[102] (1) buyers have a "last chance" to review an order before it is entered into; (2) they have a 10-day window of opportunity to withdraw from an 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 remains on the seller during the 10-day trial period after the goods have been received. Tunisian cyber-buyers enjoy some of the best protections in the world.[103]

Prohibit Computer Crimes

The following computer crimes should be outlawed: (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 can be used as a model.[104]

---

contracts, notwithstanding the fact that another statute may mandate the utilization of paper documents. This applies regardless of whether the statute creates a legal requirement, or provides for detrimental consequences if paper documents are not used. However, in order for E-documents to be used in the transfer of a right or obligation under a carriage contract, a "reliable method" must be employed to ensure the security and integrity of the message. Once data messages have begun to be used, paper documents are no longer valid. A party cannot revert to the use of paper documents until the other party has been informed that, henceforth, paper documents are to be used instead of data messages. Reversion to paper documents will not affect the rights of the parties which were created with E-documents. If a legal regulation exists in reference to paper documents relating to a carriage contract, that regulation will also be applied to a digital message used *in lieu* of paper documents. Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES (13 January 1999), art. 26 and 27, Official Translation No. 7 by Maria del Pilar Mejia de Restrepo; http://www.qmw.ac.uk/~t16345/colombia_en_final.htm.

[101] Uniform Law Conference of Canada, UNIFORM ELECTRONIC COMMERCE ACT (1999), ss 24-25; http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1&print=1.

[102] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW (hereinafter "Electronic Commerce Law" or "ECL"), 2000; http://www.bakernet.com.org. *See* Stephen E. Blythe, Note 82 supra.

[103] 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 (hereinafter "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. Furthermore, the CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of 31 March 2005; these amendments became effective on 1 April 2006. For a thorough analysis of the CPA, *see* Stephen E. Blythe, Note 80 supra. Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Stephen E. Blythe, Note 76 supra.

[104] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993; http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A. *See* Stephen E. Blythe, Note 66 supra.

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.[105]

Promote "Cybersuites"

The governments of economically underdeveloped nations such as Armenia need to constantly be on the lookout for new sources of revenue. Accordingly, Armenia should consider the promotion of "cybersuites" *a la* the Republic of Vanuatu. Vanuatu enacted its E-Business Act ("EBA") to regulate E-commerce websites which have been rented by international business firms looking for a tax haven.[106] The EBA creates an Internet Free Trade Zone whereby individuals and firms can consummate E-commerce transactions while taking advantage of Vanuatu's low business income tax rates. Vanuatu-based websites—referred to as "cybersuites" in the EBA—are rented to foreign parties so that they may engage in E-commerce without the necessity of establishment of a formal international corporation with directors, shareholders and a registered office. Cybersuite proprietors are provided assistance in the creation of the website and its maintenance.[107]

Assert Long-Arm Jurisdiction
Against Foreign Parties

Because so many of the E-commerce transactions incurred by the residents of Armenia will be with parties outside the borders of Armenia, it would be prudent for the EDL to explicitly state its claim of "long arm" jurisdiction against any E-commerce party who is

---

[105] Kingdom of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71. The original version, in Nepalese Language, is available at the website of the Nepal Telecommunications Authority: http://www.nta.gov.np/cyber_law.html. 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 60 supra.

[106] Republic of Vanuatu, E-BUSINESS ACT (Act No. 25 of 2000), Preamble; http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/ea2000125.html. For a discussion of the E-Business Act 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 AMENDMENT) ACT OF 2000, THE COMPANIES (E-COMMERCE AMENDMENT) ACT OF 2000: A PLAIN ENGLISH EXPLANATION, pp. 8-10; http://www.vanuatugovernment.gov.vu/government/library/Explanation%20o....
see also Stephen E. Blythe, Note 83 supra.

[107] "Vanuatu E-commerce," LOWTAX, p. 1; http://www.lowtax.net/lowtax/html/jvaecom.html.

a resident or citizen of a foreign jurisdiction, so long as that party has established "minimum contacts" with Armenia.[108] Minimum contacts will exist, for example, if a cyber-seller outside of the country makes a sale to a person in Armenia. In that situation, the computer laws of Armenia should be applicable to the foreign party because that party has had an effect upon Armenia through the transmission of an electronic message that was received in Armenia. The foreign party should not be allowed to evade the jurisdiction of the Armenian courts merely because he is not physically present in the country. After all, E-commerce is an inherently multi-jurisdictional phenomenon.

Evidentiary Admissibility of Electronic Form

The EDL should explicitly include the rebuttable presumption that an E-document will not be denied admission into evidence in court merely because of its electronic form. Colombia's Electronic Trade Law may be used as a model.[109]

SUMMARY AND CONCLUSIONS

Armenia's E-Document and E-Signature Law

Armenia's EDL is a first-generation E-signature law; only digital signatures are recognized. A Certification Authority is referred to as a "Certification Center;" no other jurisdiction uses that term. Licensure of CA's is not compulsory; a licensed CA is referred to as "accredited," but non-accredited CA's are also allowed. Conspicuously absent are E-contract provisions: attribution rules, rules related to acknowledgement of receipt, and rules governing time/ place that an electronic communiqué is deemed to have been sent/ received. No mention is made of consumer rights of E-commerce purchasers, and E-government is neither mandated nor forbidden. However, the statute does allow use of an E-signature instead of a handwritten signature, and use of an E-document to satisfy legal requirements related to writing, originality and retention.

Final Thoughts: Tweaking the EDL

Although it was an adequate first step, the EDL needs to be fine-tuned. The following amendments should be undertaken: (1) change to the third-generation of E-signature legislation by adoption of an inclusive definition of an E-signature and recognition of many types of E-signatures, while continuing to give the digital signature most-favored-status; (2) add a rebuttable presumption of legal admissibility of an E-document and an E-signature in a court of law; (3) add explicit long-arm jurisdiction; (4) add a provision

---

[108] 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 83 supra.
[109] Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES, 13 January 1999, art. 10; The Official English Translation No. 7 (translator: Maria del Pilar Mejia de Restrepo) is available at http://www.qmw.ac.uk/~t16345/colombia_en_final.htm .

allowing cybersuites; (5) establish information technology courts; (6) add a comprehensive list of computer crimes; (7) add E-contract rules, including rules for carriage contracts; and (8) add consumer protections for E-commerce buyers.