Annual Survey of International & Comparative Law

Volume 17 | Issue 1 Article 6

2011

A Critique of Argentine E-Commerce Law and Recommendations for Improvement

Stephen E. Blythe

A Critique of Argentine E-Commerce Law and Recommendations for Improvement

Cover Page Footnote
17 Annual Survey of Int'l. & Comp. L. 75 (2011)

A CRITIQUE OF ARGENTINE E-COMMERCE LAW AND RECOMMENDATIONS FOR IMPROVEMENT

STEPHEN E. BLYTHE*

ABSTRACT

Argentina has been experiencing rapid growth in internet accessibility and E-commerce, but its E-commerce laws need to be updated. The nation enacted a Digital Signature Law ("DSL") in 2001. Digital signatures and documents are valid in Argentina if they meet stringent security requirements and can be used to comply with legal requirements for: a handwritten signature; a paper document; an original paper document; and retention of a paper document. A digital certificate must be issued by a licensed certification authority ("CA") and must accurately identify the subscriber. The CA will issue a private key to the subscriber with the certificate, and the CA must revoke the certificate if security is compromised. CA's are licensed and regulated by the federal government and may be audited and sanctioned for legal violations.

* Professor of Business Law, College of Business Administration, Abu Dhabi University, Abu Dhabi, United Arab Emirates. E-Mail: ecommercelaw@hotmail.com. Ph.D. (Info. Tech. Law), The University of Hong Kong (China), 2010; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Glasgow, Scotland U.K.), 2005; LL.M. (Int'l Bus. Law), University of Houston, 1992; J.D. *cum laude*, Texas Southern University, 1986; Ph.D. (Business Administration), University of Arkansas, 1979; M.B.A., Arkansas State University, 1975. Attorney at Law, Texas and Oklahoma; Certified Public Accountant, 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 twelve universities located in the United States, Africa and the Middle East.

CA's may be responsible for damages incurred by third parties due to the CA's acts or omissions. Exemplary attributes of this law include: (1) mandatory licensing of CA's; (2) the rights and responsibilities of subscribers; (3) mandatory E-government with free CA service; and (4) the authorization of Registration Authorities to work for CA's in the processing of applications for certificates. The DSL provides a satisfactory legal foundation for Argentine E-commerce, but it needs to be calibrated and supplemented. Recommended changes and additions to Argentine E-commerce law include: (1) enactment of a comprehensive Electronic Transactions Law which will incorporate all laws pertinent to E-commerce, including E-contract rules; (2) recognition of the validity of the electronic form in compliance with several additional requirements of other statutes, including notarization; (3) deletion of all exclusions from coverage, which will potentially allow E-signatures and E-documents to be used in all situations; (4) addition of rules for electronic automated contracts and electronic carriage contracts; (5) addition of consumer protections for E-buyers; (6) establishment of Information Technology Courts for resolution of E-commerce disputes; (7) creation of long-arm jurisdiction over foreign E-commerce parties; (8) licensing of the Argentine Post Office as a CA; (9) adoption of a National ID Card containing a digital signature which can be activated by a CA, including the Post Office; (10) enactment of computer crimes, including Intentional Injection of a Virus into a Computer System; and (11) enactment of a third-generation E-signature law to replace the first-generation DSL.

INTRODUCTION

Argentina's internet accessibility and E-commerce have experienced a moderate amount of symbiotic growth in recent years. The Argentine E-commerce statutes have been a positive factor in attainment of E-commerce growth. However, in order to maximize growth in E-commerce, the E-commerce statutes should be amended by: improving the E-contract rules; adding consumer protections for E-commerce buyers; recognizing the long-arm jurisdiction of the statute; adding several new computer crimes; recognizing the legal validity of all types of electronic signatures; and by making several other important changes. These changes would: strengthen an E-commerce participant's contractual rights; afford greater legal protections to E-buyers; reduce the likelihood of computer fraud; facilitate the growth of international E-commerce via recognition of legal validity of all types of E-signatures; and have several other important ramifications.

The objectives of this article are to: (1) consider the recent growth of internet accessibility and E-commerce in Argentina; (2) discuss the basic

aspects of electronic signatures, public-key-infrastructure technology, and certification authorities; (3) describe the three generations of electronic signature law; (4) analyze Argentina's digital signature law and regulations; and (5) make recommendations for refinement of Argentine E-commerce law. To achieve those objectives, the article is organized into six parts: Part I, Background of Argentine E-Commerce; Part II, Technical Framework of E-Commerce; Part III, Three Generations of Electronic Signature Law; Part IV, Argentina's Digital Signature Law and Digital Signature Regulations; Part V, Recommendations for Improvement of Argentine E-commerce law; and Part VI, Conclusions.

I. BACKGROUND OF ARGENTINE E-COMMERCE

Argentina's internet accessibility has been growing in recent years. According to the CIA, 11.2 million Argentinians, in a population of approximately 40 million accessed the internet in 2008.[1] This is an internet penetration rate of 28 percent, which ranks 28th in the world.[2] However, a *Forbes* article in the same year contended that Argentina's internet penetration rate was much higher at 39.7%, second only to Chile in South America.[3] In 2009, Argentina had 4.9 million internet hosts, a world ranking of 16th.[4] In South America, only Chile has a greater degree of broadband penetration than Argentina.[5] Broadband growth has been strong since 2004.[6] Although only 800,000 in the country had access to broadband in 2005, by 2009 that number had grown to over 4 million.[7] The Argentine broadband market is divided almost equally among three companies.[8] Buenos Aires is considered one of the "most wired" cities of South America.[9]

---

1. U.S. Central Intelligence Agency, THE WORLD FACTBOOK, *Argentina*, https://www.cia.gov/library/publications/the-world-factbook/geos/countrytemplate_ar.html (Dec. 27, 2009).

2. *Id*.

3. Sramana Mitra, *Latin America's E-Commerce Leader*, FORBES, http://www.forbes.com/fdc/welcome_mjx.shtml (Mar. 21, 2008).

4. *Argentina*, *supra* n.1, at 12.

5. *Argentina—Convergence, Broadband & Internet Market—Overview, Statistics & Forecasts*, RESEARCH AND MARKETS, http://www.researchandmarkets.com/reportinfo.asp?report_id=1031104 (Apr. 2009).

6. *Argentina Internet: Broadband Takes Off*, GLOBAL TECHNOLOGY FORUM, http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=7624&title=Argentina+internet%3A+Broadband+takes+off&channelid=4&categoryid=28 (Sept. 5, 2005).

7. *Communications in Argentina*, *supra* n. 4.

8. *Argentina—Convergence, Broadband & Internet Market—Overview, Statistics & Forecasts*, *supra* n. 6.

9. Anil Mundra, *Argentina's Wired City*, GLOBAL POST, http://www.globalpost.com/print/3503198 (Sept. 11, 2009).

With the availability of the internet, Argentine E-commerce has begun to flourish. The rise in the number of broadband connections has made E-transactions quicker and easier to consummate. Argentina became the E-commerce leader in the Spanish-speaking world in 2007.[10] Argentina also produces half of the internet's Spanish-language E-commerce websites and has 11 of the top 15 E-commerce websites in terms of traffic in Latin America and Spain.[11] The E-commerce growth rate was 120% in 2005 and 100% in 2006.[12] In 2010, the growth rate is expected to show signs of maturity but is still expected to be in the respectable range of 25 to 30%.[13]

II. TECHNICAL FRAMEWORK OF E-COMMERCE

Part II provides general technical background information which will facilitate attainment of an understanding of the Argentine E-commerce statutes. The following issues are covered: basic aspects of E-signatures; four levels of online security; public key infrastructure; advantages and disadvantages of the digital signature; and the critical role of the certification authority whenever a digital signature is used.

A. ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[14] 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,"[15] 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."[16] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin

10. *Argentina: Overview of E-Commerce*, GLOBAL TECHNOLOGY FORUM, http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=11158&title=Argentina%3A+Overview+of+e-commerce&channelid=4&categoryid=27 (Aug. 1, 2007).

11. *Id*.

12. Juan Pedro Tomas, *E-Commerce Expected to Grow 100% This Year—Argentina,* BUSINESS NEWS AMERICAS, http://www.bnamericas.com/news/technology/Cace:_E-commerce_expected_to_grow_100*_this_year (June 30, 2006).

13. Juan Pedro Tomas, *E-Commerce Expected to Expand 25-30% as Internet Users Mature*, BUSINESS NEWS AMERICAS, http://www.bnamericas.com/news/technology/E-commerce_expected_to_expand_25-30*_this_year_as_internet_users_mature (Jan 13, 2010).

14. *See e.g.,* U.C.C.§ 2-201, 2-209 (1977).

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

16. 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.

number, a digitized image of a handwritten signature attached to an electronic message, or merely a name typed at the end of an e-mail message.[17]

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."[18] 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. There are four levels of security used in E-commerce.

B. ONLINE CONTRACTS: FOUR LEVELS OF SECURITY

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

The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[19]

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.[20]

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,[21] 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

17. David K.Y. Tang, *Electronic Commerce: American and International Proposals for Legal Structures*, REGULATION AND DEREGULATION: POLICY AND PRACTICE IN THE UTILITIES AND FINANCIAL SERVICES INDUSTRIES 333 (Christopher McCrudden ed., 1999).

18. Michael Dessent, *Browse-Wraps, Click-Wraps and Cyber Law: Our Shrinking (Wrap) World*, 25 T. JEFFERSON L. REV. 1, 4 (2002).

19. Jonathan E. Stern, Note, *Federal Legislation: The Electronic Signatures in Global and National Commerce Act*, 16 BERKELEY TECH. L.J. 391, 395 (2001).

20. *Id*.

21. In the highly successful Hong Kong Identity Card, the two thumb prints are used as a biometric identifier. See, Rina C.Y. Chung, *Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PACIFIC L. & POL'Y J. 442 (2003).

from the person in advance and stored for later comparison with a person purporting to have the same identity.[22] 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.[23]

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;"[24] 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.[25] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[26] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[27]

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.[28] It is "the sequence of bits that is created by running an

22. Stern, *supra* n. 20, at 395-96*; see also The Legality of Electronic Signatures Using Cyber-Sign is Well Established*, CYBER-SIGN, http://www.cybersign.com/news news.htm.

23. *Id*.

24. K.H. Pun, Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan, *Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?,*32 HONG KONG L.J. 241, 256 (2002).

25. *Id*. at 257.

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

27. *supra* n. 22.

28. 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

electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key."[29] 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.[30] These two advantages are the result of the technology employed by the digital signature—public key infrastructure.

C. DIGITAL SIGNATURE TECHNOLOGY: PUBLIC KEY INFRASTRUCTURE

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI."[31] PKI consists of four steps:

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.[32]

The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it.[33] A "hash value" is created by applying a "hash function"—a standard mathematical function—to the contents of the electronic document.[34] 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.[35] The encrypted hash function is the "digital signature" for the document.[36]

The third step is to attach the digital signature to the message and to send both to the recipient.[37]

The fourth step is for the recipient to decrypt the digital signature by using the sender's public key.[38] If decryption is possible the recipient

---

Special Autonomous Region, ELECTRONIC TRANSACTIONS ORDINANCE, Ord. No. 1 of 2000, s 2.

29. Smedinghoff, *supra* n. 16, at 146.

30. Christopher T. Poggi, *Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation*, 41 VA. J. INT'L L. 224, 250-51 (2000).

31. Susanna Frederick Fischer, *California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, 7 B.U. J. SCI. & TECH. L. 229, 233 (2001).

32. Pun, *supra* n.25, at 249.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

knows the message is authentic, i.e., that it came from the purported sender.[39] Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest.[40] If they match, the recipient knows the message has not been altered.[41]

PKI gives the digital signature several unique advantages over other types of E-signatures.

D. 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." [42] Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific." [43]

The digital signature is the only form of electronic signature satisfying all three of the UNCITRAL evaluation factors, i.e., that an electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud.[44] 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.[45]

Despite those significant advantages, the digital signature has potential pitfalls.

---

38. *Id.*
39. *Id.*
40. *Id.*
41. Jochen Zaremba, *International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers*, 18 CONN. J. INT'L L. 479, 512 (2003).
42. Pun, *supra* n. 25, at 250.
43. *Id*.
44. *Id.* at 243.
45. *Id.* at 252.

E. DISADVANTAGES OF THE DIGITAL SIGNATURE

The digital signature has at least two drawbacks. Firstly, the private key of each person is rather difficult to memorize, and 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 for 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.[46]

The other disadvantage of the digital signature pertains to the digital certificate, which must be issued by a Certification Authority ("CA").[47] 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.[48] Because the CA is so essential to the success of the digital signature, it is important for the user to understand exactly what the CA does and why its role is so critical.[49]

F. 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.[50] 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.[51] 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[52]—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[53]

---

46. *Id.* at 253.
47. *Id.*
48. *Id*.
49. *Id.*
50. Hogan, *infra* n. 54.
51. Hogan, *infra* n. 54.
52. Certification Authority ("CA") is the term used in this article because it seems to be the most commonly used designation around the world.
53. Tara C. Hogan, *Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?*, 4 N.C. BANKING INST. 417, 424-25 (2000).

The most important job of the CA is to issue certificates confirming basic facts about the subscriber, the subject of the digital certificate. Of course, the certificate is a digitized, computer-held, record containing the most pertinent information about a transaction between two transacting parties. Typical information contained in a certificate includes the following: the name and address of the CA that issued the certificate; the name, address and other attributes of the subscriber; the subscriber's public key; and the digital signature of the CA.[54] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[55]

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 corresponding to the public key. This is done without disclosing the specifics of the private key.[56] The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered by the particular CA. Ordinarily, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued.[57]

In order to indicate the authenticity of the digital certificate, the CA will sign it with her digital signature. Ordinarily, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties who 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.[58]

One of the recurring problems for lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber. Nations around the world, as well as individual states in the

54. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 58 (1996).
55. Hogan, *supra* n. 42, at 425-426.
56. Smedinghoff, *supra* n. 16, at 149.
57. *Id.* at 150.
58. Hogan, *supra* n. 42, at 426-27.

U.S., 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 with dissimilar digital signature laws.[59]

A digital certificate is only as reputable as the CA who issued it. If the CA is unreliable and untrustworthy, the digital certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate.[60]

III. THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

E-signature law has evolved quickly since the 1990s. In this part, its three generations are covered: first generation, which only recognized one type of E-signature—the digital signature; second generation, which recognized all types of E-signatures; and third generation, which recognizes all types of E-signatures, but gives a preference for the digital signature.

A. 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.[61] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[62] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature include Bangladesh,[63] India,[64]Malaysia,[65] Nepal,[66] New Zealand[67] and

59. Andrew B. Berman, Note, *International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures*, 28 SYRACUSE J. INT'L L. & COM. 125, 143-44 (2001).

60. David Hallerman, *Will Banks Become E-commerce Authorities?*, 12 BANK TECH. NEWS, June 1, 1999.

61. Utah Code Ann. § 46-3-101 *et seq.* (1995). This first-generation statute was repealed in 2000 and replaced with the Uniform Electronic Transactions Act, a second-generation model law. Utah Code Ann. § 46-4-101 *et seq.* (2000), http://le.utah.gov/~code/TITLE46/46_04.htm. *See E-Commerce and E-Signature Law of the United States of America, infra* n. 60.

62. *Id.*

63. Bangladesh, INFORMATION TECHNOLOGY (ELECTRONIC TRANSACTION) ACT ("ITA") (Draft), http://www.bangladeshgateway.org/lawit.pdf (2000).

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

65. Republic of Malaysia, DIGITAL SIGNATURE ACT ("DSA"),

Russia.[68] Argentina, the subject of this paper, also has a first-generation statute.[69]

Unfortunately, first-generation jurisdictions have often discovered that their recognition of only one form of technology is burdensome and overly restrictive. Frequently, they have observed that forcing all users to employ a digital signature gives them more security, but that this benefit is outweighed by the digital signature's disadvantages: e incurrence of certification authority fees; inconvenience of being forced to use a certification authority; other types of E-signatures might be better suited to a particular type of transaction; PKI may be less adaptable to technologies used in other nations, or even by other persons within the same nation; inappropriate risk allocation between users if fraud occurs; and the potential disincentive to invest in development of alternative technologies.[70]

B. THE SECOND WAVE: TECHNOLOGICAL NEUTRALITY

Jurisdictions in the Second Wave overcompensated by recognizing the legal validity of all types of E-signatures.[71] They did the complete reversal of the First Wave and did not include any technological restrictions whatsoever in their statutes.[72] 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.[73] These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend

---

http://www.mycert.org.my/bill/digisign/digi1.html (1997).

66. Federal Democratic Republic of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), § 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 (2005). *See* Stephen E. Blythe, *On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law*, 8:1 JOURNAL OF HIGH TECHNOLOGY LAW (2008), a publication of Suffolk University School of Law, Boston, Massachusetts USA.

67. New Zealand, ELECTRONIC TRANSACTIONS ACT 2000, http://www.med.govt.nz/templates/MultipageDocumentPage____9779.aspx.

68. Russian Federation, ELECTRONIC DIGITAL SIGNATURE LAW, Federal Law No. 1-FZ, 10 January 2002. *See* Fischer, *supra* n. 32, at 234-37.

69. *See* Argentine Republic, *infra.* n. 92.

70. Amelia H. Boss, *The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce*, 34:3 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673, 689-90 (2009). It is debatable as to whether technological-neutrality or technological-specificity is the correct road to take. *See* Sarah E. Roland, Note, *The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?,* 35 SUFFOLK U. L. REV. 625, 638-45 (2001).

71. Fischer, *supra* n. 32, at 234-37.

72. *Id.*

73. *Id.*

that any one of them is necessarily better than the others.[74] In other words, they are "technologically neutral."[75] Permissive jurisdictions provide legal recognition of many types of electronic signatures and do not grant a monopoly to any one of them.[76] The United States of America[77] is a member of the second wave; the overriding majority of its jurisdictions (forty-five states, the District of Columbia, and the Territories of Puerto Rico and Virgin Islands) have enacted the Uniform Electronic Transactions Act (either in its entirety or with minor amendments), which is a permissive second-generation model law.[78] Australia has also enacted a second-generation statute.[79]

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

C. THE THIRD WAVE: A HYBRID

The Third Wave was characterized by a recognition of the legal validity of all types of E-signatures, but with a preference for the digital signature. Singapore was in the vanguard of this generation. In 1998, this country adopted a compromised, 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.[80] In terms of relative degree of technological

---

74. *Id.*
75. *Id.*
76. *Id.*
77. For analysis of American law, *see E-Commerce and E-Signature Law of the United States of America*, THE UKRAINIAN JOURNAL OF BUSINESS LAW, Kiev, Ukraine (Nov., 2008). For concise coverage of American, British, E.U. and U.N. 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).
78. United States of America, National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 20 (Supp. 2000), http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm. The State of Washington is the only U.S. jurisdiction presently having a first-generation statute, and these states have third-generation statutes: Alabama, Georgia, Florida and Ohio. *See also* United States of America, ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT ("E-Sign"), Public Law 106-229, 15 U.S.C. 7001, 114 Stat. 464, http://www.esignrecords.org/resources/esign.pdf (June 30, 2000).
79. Commonwealth of Australia, ELECTRONIC TRANSACTIONS ACT, http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/ (1999). *See* Fischer, *super* n. 32, at 234-37.
80. United Nations Commission on International Trade Law ("UNCITRAL"), MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT (hereinafter "MLEC"), G.A.

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 tie itself to one form of technology. 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 allows parties to more easily consummate electronic transactions with parties from other nations.[81]

In recent years, more and more nations have joined the Third Wave. They recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures. This preference is exhibited in several ways: (1) utilization of a digital signature using a PKI system is explicitly required for authentication of an electronic record; (2) utilization of a digital signature with PKI seems to be necessary in order for an electronic record to comply with any statutory requirement that a record be in paper form; and (3) in order for a signature in electronic form to comply with a statutory requirement that a pen-and-paper signature be affixed, it must be a digital signature created with PKI. Nevertheless, the Third Wave jurisdictions do not appear to be as technologically-restrictive as those in the First Wave. They do not compel the E-commerce participant to use only the digital signature, *in lieu* of other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

The moderate position adopted by Singapore has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European Union's E-Signatures Directive,[82] Armenia,[83] Azerbaijan[84] Barbados,[85] Bermuda,[86] Bulgaria,[87]

Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996). *See* Stephen E. Blythe, *supra* n. 60, second citation.

81. Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88) ("ETA"), 10 July 1998; Although granting legal recognition to most types of electronic signatures, the Singapore statute implicitly makes a strong suggestion to users that they should use the digital signature because it is more reliable and more secure than the other types of electronic signatures in two ways: (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. *See* Stephen E. Blythe, *Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality*, 33 OHIO NORTHERN UNIVERSITY LAW REVIEW 525-562 (2006).

82. European Union Directive, *supra* n. 17; *see* Stephen E. Blythe, *supra* n. 60, second citation. For concise coverage of European Union law, *see* Stephen E. Blythe, *E-Signature Law and*

Burma,[88] China,[89] Colombia,[90] Croatia,[91] Dubai,[92] Finland,[93] Hong Kong,[94] Hungary,[95] Iran,[96] Jamaica,[97] Japan,[98] Lithuania,[99] Pakistan,[100] Peru,[101]

E-Commerce Law of the European Union and its Member States, THE UKRAINIAN JOURNAL OF BUSINESS LAW, pp. 22-26 (May, 2008). In an assessment of the effectiveness of its E-Signature Directive in 2006, the European Commission concluded that contracting parties had been slow to use digital signatures, but that "many other simpler electronic signature applications had become available." Reasons advanced by the Commission for the slow rate of adoption of digital signatures include: "technical problems in the marketplace, a lack of criteria for certification and mutual recognition, a lack of interoperability at national and cross-border levels, and the existence of isolated areas where certificates were used for a single purpose." Overall, the primary reason advanced was an economic one, caused by a typical user's decision to eschew development of a multi-application digital signature in favor of an E-signature which is applicable to its own industry, e.g., the banking sector. REPORT ON THE OPERATION OF DIRECTIVE 1999/93/EC ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES, s 5.2, COM (2006), cited in Boss*, supra* n. 59, at 695-96. Despite the less than enthusiastic reception of the digital signature in Europe and elsewhere, that rate of acceptance is expected to be given a "shot in the arm" felt worldwide by the "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (hereinafter "Rotterdam Rules")", http://www.unis.unvienna.org/unis/pressrels/2008/unisl125.html. The Rotterdam Rules became effective on 23 September 2009 and recognize the legal validity of electronic bills of lading. In order to comply with the security requirements of Article 38 of the Rotterdam Rules, it will apparently be necessary to employ a digital signature. Felix W.H. Chan, *In Search of a Global Theory of Maritime Electronic Commerce: China's Position on the Rotterdam Rules*, 40 JOURNAL OF MARITIME LAW AND COMMERCE 185 (2009). *See also* Manuel Alba, *Electronic Commerce Provisions in the UNCITRAL Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea*, 44 TEXAS INTERNATIONAL LAW JOURNAL 387 (2009). Accordingly, *a la* Mark Twain's rumored death, any notion that the digital signature is passé appears to have been "greatly exaggerated." The digital signature appears to have a bright future because, presently at least, it is the epitome of security.

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

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

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

86. Commonwealth of Bermuda, ELECTRONIC TRANSACTIONS ACT 1999 ("ETA"); http://www.bakernet.com/ecommerce/bermuda-eta.doc.*See* Note 18 supra at 234-37.

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

88. The Union of Myanmar, ELECTRONIC TRANSACTIONS LAW ("ETL"), The State Peace and Development Council Law No. 5/2004, The 12 Waxing of Kason 1366 M.E., , http://ibiblio.org/obl/docs/Electronic-transactions.htm (Apr. 30, 2004). *See* Stephen E. Blythe, *Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As a Sign Of Hope For a Troubled Nation*, 3:1 INTERNATIONAL BUSINESS RESEARCH __ (2010), a publication of the

Canadian Center of Science and Education, Toronto, Canada, http://ccsenet.org/journal/index.php/ibr/ (2010).

89. People's Republic of China, Order No. 18 of the President, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, Promulgated 28 August 2004, Effective 1 April 2005. The statute was translated into English by the Beijing University School of Law, Beijing, China, and is available (by subscription only) at their website: http://www.lawinfochina.com/dispecontent.asp?db=1&id=3691. *See* Stephen E. Blythe, *China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce*, 7 CHICAGO-KENT JOURNAL OF INTELLECTUAL PROPERTY 1 (2007), a publication of Chicago-Kent College of Law, Illinois Institute of Technology, Chicago, Illinois USA. *See also* Felix W.H. Chan, *E-Commerce All at Sea: China Welcomes Digital Bills of Lading Under the Electronic Signature Law 2005*, 3 OKLAHOMA JOURNAL OF LAW AND TECHNOLOGY 31 (2006).

90. Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES ("ETL"), Official Translation No. 7 by Maria del Pilar Mejia de Restrepo, http://www.qmw.ac.uk/~t16345/colombia_en_final.htm (Jan. 13, 1999). *See* Stephen E. Blythe, *Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act*, a book chapter in INTERNET POLICIES AND ISSUES, Frank Columbus, Editor, Nova Science Publishers, Inc., New York NY USA, 2009.

91. Republic of Croatia, ELECTRONIC SIGNATURE ACT ("ESA") (Jan. 17, 2002), http://www.ehrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/00/document/eSignatureAct OG10_2002.pdf. *See* Stephen E. Blythe, *Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security*, 26: 1 EUROPEAN JOURNAL OF LAW AND ECONOMICS 75-103 (Aug., 2008), a publication of Springer Netherlands Ltd., Amsterdam.

92. Emirate of Dubai, LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE NO. 2/2002 ("ETL"), 12 February 2002; http://www.tecom.ae/law/law_2.htm. *See* Stephen E. Blythe, *The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries*, 22:1 JOURNAL OF ECONOMICS AND ADMINISTRATIVE SCIENCES 103 (2007).

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

94. Hong Kong Special Autonomous Region, People's Republic of China, ELECTRONIC TRANSACTIONS ORDINANCE, Ordinance No. 1 of 2000. 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 enacted, 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), a publication of the University of North Carolina School of Law, Chapel Hill, NC USA.

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

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

97. Jamaica, ELECTRONIC TRANSACTIONS ACT, 2005. *See* Stephen E. Blythe, *Internet Law As A Potential Catalyst For Growth Of Caribbean E-Commerce: Jamaica's Statute As A Model*, a paper presented and published in the READINGS BOOK OF THE ACADEMY OF

Slovenia,[102] South Korea,[103] Taiwan,[104] Tunisia,[105] United Arab Emirates,[106] Vanuatu[107] and in the proposed statute of Uganda.[108] Many

---

BUSINESS ADMINISTRATION GLOBAL TRENDS CONFERENCE, Cancun, Mexico, (Dec. 19-22, 2009).

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

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

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

101. Republic of Peru, LAW REGULATING DIGITAL SIGNATURES AND CERTIFICATES, translated by National Law Center for Inter-American Free Trade, http://natlaw.com/interam/ar/ec/tn/tnarecl.htm (May 28, 2000). *See supra* n. 56.

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

103. Korean Legislation Research Institute, DIGITAL SIGNATURE ACT NO. 5792, *Statutes of the Republic of Korea,* Vol. 16 (II), pp. 1217-1220 (1999). The statute has been amended two times: (1) Act No. 6360 of 16 January 2001; and (2) Act. No. 6585 of 31 December 2001. *See* Stephen E. Blythe, *The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation*, 28: 3 HOUSTON JOURNAL OF INTERNATIONAL LAW 573-661 (2006), a publication of the College of Law, University of Houston, Houston, Texas USA.

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

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

106. United Arab Emirates, FEDERAL LAW NO. (1) OF 2006 ON ELECTRONIC COMMERCE ANDTRANSACTIONS ("ECL"), http://www.tra.ae/pdf/legal_references/Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf (30 January 2006). *See* Stephen E. Blythe, *The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate*, a paper presented and published in the PROCEEDINGS OF THE ANNUAL INTERNATIONAL CONFERENCE ON GLOBAL BUSINESS, Dubai, United Arab Emirates, May 10-13, 2009.

other nations are either currently using the hybrid approach or are considering the adoption of it.

IV. ARGENTINA'S DIGITAL SIGNATURE LAW

The Argentine Republic enacted its Digital Signature Law (hereinafter "DSL") in 2001[109] and its Digital Signature Regulations in 2002.[110] The purpose of Part IV is to summarize the DSL and the DSR and to set the stage for Part V, which will generate several recommendations for improvement of those laws.

EXCLUSIONS

Electronic documents and electronic signatures may not used in: (1) wills; (2) family law documents (e.g., marriage licenses and divorce decrees); (3) "private acts in general;" (4) situations where existing law prohibits the use of them; and (5) situations where the parties have agreed not to use them.[111] In all of those situations, the electronic form is not legally valid and paper documents must be used.

---

107. Republic of Vanuatu, ELECTRONIC TRANSACTIONS ACT, (Act. 24 of 2000) http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/eta2000256.html. The E-commerce law of the Commonwealth of Bermuda was used as a model for this statute. "Vanuatu E-commerce," LOWTAX, 1, http://www.lowtax.net/lowtax/html/jvaecom.html. For a discussion of the ETA by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—*see* Hon. Prime Minister Barak T. Sope Maautamate, MP, Government of the Republic of Vanuatu, *The e-Business Act of 2000, The International Companies (E-Commerce Amendment) Act of 2000, The Companies (E-Commerce Amendment) Act of 2000: A Plain English Explanation*, 3-7, http://www.vanuatu.gov.vu/government/library/Explanation%20of%20the%20ecommerce%20acts.htm (2000).

See also Stephen E. Blythe, *South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga*, 10: 1 JOURNAL OF SOUTH PACIFIC LAW (2006), a publication of the School of Law, University of the South Pacific, Emalus Campus, Port Vila, Republic of Vanuatu.

108. Republic of Uganda, ELECTRONIC SIGNATURES ACT (Draft), http://www.sipilawuganda.com/downloads/electronic%20signatures%20bill%202004.pdf (2004). *See* Stephen E. Blythe, *The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control*, a paper to be presented and published in the PROCEEDINGS OF THE TENTH ANNUAL CONFERENCE OF THE INTERNATIONAL ACADEMY OF AFRICAN BUSINESS AND DEVELOPMENT, Kampala, Uganda, (May 19-23, 2009).

109. Argentine Republic, DIGITAL SIGNATURE LAW 25.506 (hereinafter "DSL"),, http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm (Dec.11, 2001).

110. Argentine Republic, DIGITAL SIGNATURE DECREE 2628/2002 (hereinafter "DSR"), http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/80733/norma.htm (Dec. 19, 2002). The original DSR was amended by DIGITAL SIGNATURE DECREE 724/2006 on June 8, 2006 (hereinafter "DSA"), http://infoleg.mecon.gov.ar/infolegInternet/anexos/115000-119999/116998/norma.htm. These statutes and other related information are available for perusal by the general public at the digital signature website maintained by the Argentine government at: http://www.pki.gov.ar/index.pho?lang=en.

111. DSL art. 4.

SELECTED DEFINITIONS

The DSL provides that security standards used with digital signatures must be in accordance with "current international technological standards"[112] and must allow for third party verification, the identification of the signatory, and detection of any alteration of the communiqué. A digital signature is defined to be "the result of applying a mathematical procedure to a digital document, that requires information controlled exclusively by the signing party and which is under his absolute control."[113] An electronic signature is defined as "a set of integrated electronic data, linked or associated logically to other electronic data, used by the signing party as his means of identification, which lacks any of the necessary requirements to be considered a digital signature."[114] If a party uses an "unrecognized" type of electronic signature (i.e., one that is not a digital signature), the burden is upon that party to prove its validity.[115] Hence, the Argentine DSL is a first-generation statute.

REQUIREMENTS FOR VALIDITY OF A DIGITAL SIGNATURE

A digital signature has full legal validity if the following requirements are met: (1) creation during the period of validity of the digital certificate; (2) verification by use of the proper confirmation procedure using the data in the certificate; and (3) the certificate was issued by a licensed Certification Authority ("CA").[116] Because the DSL is first-generation, the digital signature is the only type of E-signature which can meet these requirements; other types of E-signatures will not be accorded full legal validity.

USE OF ELECTRONIC FORM TO SATISFY REQUIREMENTS IMPOSED BY OTHER LAWS

Whenever another law requires the presence of a handwritten signature to incur a legal right (or the incurrence of a legal detriment if the handwritten signature is absent), that requirement may be met with a valid digital signature.[117] Whenever another law requires the presence of a written document to incur a legal right, that requirement may be met with a digital document.[118] Whenever another law requires the presentation of an original document in order to incur a legal right, that

112. DSL art. 2.
113. *Id.*
114. DSL art. 5.
115. *Id.*
116. DSL art. 9.
117. DSL art. 3.
118. DSL art. 6.

requirement may be met with presentation of a digital document signed with a digital signature.[119] Whenever another law requires the retention of a paper document, that requirement is met by the retention of a digital document, so long as the document may be retrieved at a later time and the following information may be ascertained: the document's point of origination, destination, date and hour of creation, date and hour mailed, and date and hour received.[120]

LEGAL PRESUMPTIONS

A digital signature is presumed to be that of the holder of the digital certificate that attests to it.[121] If the verification procedure confirms the authenticity of the digital signature, it is presumed that the digital document attached to the digital signature has not been altered after the signature was attached.[122] If a digital document has been signed with a digital signature and has been sent by a person's automatically programmed device, it is presumed that the document was sent by the person in question.[123]

DIGITAL CERTIFICATES

A digital certificate links the signature verification data to its holder.[124] The following are legal requirements for validity of a digital certificate: (1) issuance by a licensed CA; and (2) adherence to an internationally recognized format which allows identification of the subscriber and the issuing CA, verification of any revocation status, differentiation between verified and non-verified information in the certificate, confirmation of the authenticity of the signature, and identification of the CA's certification policy.[125] The digital certificate must state its period of validity, and this period cannot extend beyond the expiration date of the CA's license.[126] A digital certificate issued by a foreign CA may be recognized in Argentina if: (1) there is a reciprocity agreement between Argentina and the foreign country in which the CA resides, and the foreign country's security standards are comparable to that of Argentina or (2) an Argentine CA recognizes a digital certificate issued by a foreign

119. DSL art. 11.
120. DSL art. 12.
121. DSL art. 7.
122. DSL art. 8.
123. DSL art. 10.
124. DSL art. 13.
125. DSL art. 14.
126. DSL art. 15.

CA and guarantees its validity, and the Argentine government validates the recognition.[127]

CERTIFICATION AUTHORITIES

A certification authority ("CA") is defined as "any person, public registry of contracts or a government agency which issues certificates and renders other services related to digital signatures and holds a license for this purpose…"[128] Argentina has a compulsory system of CA licensing; every CA is required to have a license.[129] CA's are private enterprises[130] and set their own fees.[131] The purposes of a CA are to: (1) process applications for digital certificates[132] and to issue them if the subscriber has met the requirements; (2) maintain records of the digital certificates that have been issued and to keep copies of them; (3) inform the subscriber and the general public of the status of a digital certificate, and to revoke the digital certificate when the subscriber so requests (i.e., when false information was used to obtain it, security has been lost, when special conditions specified in the CA's certification policy are present, or when directed to do so by a court order.)[133] In order to achieve these purposes, the CA should carefully inform the subscriber of all pertinent information at the date of issuance of the certificate, including: (1) the liability of the parties; (2) the need to maintain security of the private key and the data contained in it; (3) the procedures involved in use of a digital certificate; and (4) required technical standards of the subscriber's computer system. After the digital certificate has been issued, the CA is required to post public notification of the status of the certificate at its website and to revoke a digital certificate if security has been compromised. Furthermore, the CA is expected to have sufficient technical knowledge, to hire competent personnel and to allow

127. DSL art. 16.
128. DSL art. 17.
129. DSL art. 26.
130. However, CA's are subject to regulation by the Argentine Application Authority and may be audited by that body. DSL art. 27. Additionally, the Application Authority may rely upon the advice and assistance of the Public Key Infrastructure Advisory Commission ("PKIAC"). DSL art. 28. The PKIAC consists of seven persons with pertinent experience in professional organizations, and each member serves for a five-year term, renewable only once. The PKIAC is charged to meet at least every three months, to hold public hearings on issues relating to digital signatures and CA's, and to provide advice to the Application Authority. DSL art. 35. Specific issues to be considered by the PKIAC include: technological standards, records of digital certificates that have been issued, information required to be given to the subscriber by the CA, and confidentiality of information given to the CA by the subscriber. DSL art. 36.
131. *Id.* Authorities of the Argentine government regulating professional licenses may also issue digital certificates, and if they do so they must also comply with CA requirements. DSL art. 18.
132. Digital certificates may be used only for a specified purpose. They may not be used for transactions beyond a specified value, and they may not be used after they have been revoked. DSL art. 23.
133. DSL art. 19.

government regulatory officers to enter the CA's worksite for purpose of routine and extraordinary inspection.[134] The CA's license will become invalid: (1) upon the expiration of its period of validity, unless it is properly renewed; (2) upon the request of the CA to the regulatory body; (3) if the CA loses legal capacity; or (4) if the regulatory body cancels the license.[135]

SUBSCRIBERS

A subscriber is the person to whom a digital certificate has been issued. A subscriber has the following legal rights: (1) to be informed in writing by the CA of all conditions of usage of the digital certificate; (2) to rely on the CA's technical ability and equipment to provide confidentiality of information given to the CA; (3) to be informed by the CA of the fees to be charged before the issuance of the certificate; (4) to be informed of the CA's address and the party to whom the subscriber may contact if there is a problem with the service; and (5) to receive the service contracted for and not to receive advertisements from the CA.[136] Subscribers are expected to carry out the following duties: (1) maintain security of the private key; (2) use a reliable private key; (3) request revocation of the certificate if security has been compromised; and (4) inform the CA if there has been any change in information previously given to the CA.[137] This list of rights and responsibilities of subscribers is exemplary and is recommended for adoption by other nations.

REGULATION OF CA'S

The Application Authority is the federal government agency which regulates CA's and has the following specific charges: (1) issuance of regulations necessary to implement the DSL; (2) establishment of technical standards to be used, included standards of signature creation and verification devices; (3) determination of the effects of revocation of a digital certificate; (4) creation of reciprocal agreements with foreign nations for recognition of certificates issued by foreign CA's; (5) determination of auditing standards for CA's;[138] (6) determination of the

134. DSL art. 21.
135. DSL art. 22.
136. DSL art. 24.
137. DSL art. 25.
138. An auditing fee may be assessed against the CA for pertinent expenses incurred by the Application Authority or its authorized third party. DSL art. 32. If a third party is used to conduct the audit, it should be an experienced university or scientific/technical institute. DSL art. 34. An audit should cover the following issues: reliability of the technical equipment used, security of the procedures, confidentiality of the data, and compliance with the CA's Certification Practice Statement, Security Plan and Business Continuity Plan. DSL art. 33.

amount of fines to be levied against CA's in violation of the DSL; (7) determination of categories of CA licenses; (8) issuance[139] and revocation of CA's licenses; and (9) oversight of CA's to ensure they are in adherence with the DSL.[140] Toward those ends, the Application Authority must: (1) not maintain a copy of the private key used by a CA; (2) maintain security over the private key it uses to create its own digital signature; (3) publish on its website the names and contact information of all licensed CA's; and (4) ensure that proper procedures are carried out whenever a CA's terminates its operations.[141]

LEGAL LIABILITY OF CA'S

The CA and the subscriber enter into a contract at the time of issuance of the digital certificate.[142] The CA is legally liable to third parties who are damaged due to their reliance upon the information in the digital certificate, if: (1) the CA failed to abide by the DSL; (2) the digital certificate contained false information; (3) the digital certificate was not promptly[143] revoked after the CA learned of the existence of the false information; or (4) the CA failed to use legally-required procedures.[144] However, the CA's legal liability is not absolute. The CA is not responsible for damages incurred by a third party if: (1) the digital certificate was used for a purpose expressly prohibited in the certificate, or is prohibited by law; (2) the damages were incurred because usage of the certificate was in violation of any restrictions expressed therein; or (3) if the damages occurred due to erroneous information in the certificate, and the CA is able to show that it took reasonable measures to verify the information.[145]

PUNISHMENT OF CA'S

A warning may be given to the CA if it does the following: (1) issues a certificate not containing all of the required information, but the absence of information is not so compelling as to invalidate the certificate; (2) fails to provide the regulatory authority with information that has been requested; or (3) violates another requirement of the DSL.[146]

---

139. A licensing fee may be required to be paid by the new CA. DSL art. 32.
140. DSL art. 30.
141. DSL art. 31.
142. DSL art. 37.
143. The CA carries the burden of showing that it used proper diligence. DSL art. 38.
144. DSL art. 38.
145. DSL art. 39.
146. DSL art. 41 and 42.

A fine in the amount of 10,000 pesos to 500,000 pesos[147] may be levied against a CA for: (1) violating DSL art. 21; (2) issuing certificates without complying with required procedures, and damages are thereby caused to the subscriber or third parties; (3) failing to maintain records of issued certificates; (4) failing to promptly revoke a certificate containing erroneous information; (5) refusing to cooperate with the regulatory body during an audit or inspection; or (6) failing to comply with the DSL's implementation regulations.[148]

A CA's license may be revoked for a period of ten (10) years if the CA: (1) does not take proper security measures; (2) issues a false digital certificate; (3) makes an unauthorized transfer of its license to another party, or uses the license for a fraudulent purpose; or (4) becomes bankrupt.[149]

After administrative remedies have been exhausted, a CA may appeal the punishment to the Federal Court.[150]

MANDATORY E-GOVERNMENT

Within five (5) years of the enactment of the DSL, the federal government was required to use digital documents and digital signatures in reference to all "laws, decrees, administrative decisions, resolutions and sentences…"[151] The DSR mandates the provision of E-government services with free CA services.[152] Mandatory offering of E-government services to the general public is exemplary and is recommended for adoption by other nations having the financial wherewithal to do this.

ASSESSMENT OF THE DSL

The statute is weakened by its first-generation status; the only type of E-signature that receives full legal recognition is the digital signature. However, the statute's list of rights and responsibilities of subscribers is exemplary and is recommended for adoption by other nations. Mandatory E-government with free CA services is also noteworthy and should be considered by other countries. The use of Registration Authorities by CA's to operate branch offices and to process and check

147. This corresponds to a range of approximately U.S. $2,636 to $131,787. XE.com, 14 January 2010.
148. DSL art. 41 and 43.
149. DSL art. 44.
150. DSL art. 45.
151. DSL art. 48.
152. DSL, *supra n.* 141. *See also infra* n. 142.

applications for certificates is a good idea as well because it provides more convenience to the general public.

DIGITAL SIGNATURE REGULATIONS

The DSL does not contain all of the specific detailed rules which are necessary for its implementation. The Digital Signature Regulations (hereinafter "DSR"), enacted in 2002 and amended in 2006, are designed to provide those rules.[153]

The chief of the Cabinet of Ministers is charged with the duty of establishing technical standards pertinent to the creation, transmission, and storage of E-documents.[154] He also appoints the members of the Advisory Committee for Digital Signature Infrastructure to maintain communications regarding digital signature issues among these groups: government agencies, private business firms, private users and consumer organizations.[155]

The chief of the Cabinet of Ministers appoints a Digital Signature Manager, who is responsible for the licensure, regulation and administration of Certification Authorities ("CA").[156] Licensing requirements of CAs are specified; the licensing period is for five (5) years and it may be renewed.[157] To be licensed, a prospective CA must show that it possesses twelve (12) types of resources.[158] CA's are required to use equipment which complies with stringent technological standards.[159]

The required contents of certificates are specified.[160] A CA must follow specific guidelines relating to the identification of subscribers and the

153. Japan, *supra* n. 81.

154. DSR, *supra* n. 91 art. 4-6 (second citation).

155. DSR art. 7-10. The members serve *pro bono* and must be qualified in terms of relevant experience and/or education. *Id.* In 2009, the President of Argentina created the Multisectorial Task Group for the purpose of fostering the "use of information and communication technologies, incorporating all the levels of the public sector, civil society and scientific academic sector to propose policies and actions intended to have access and make use of [those technologies] as elements of social development, and facilitate the local production of goods and services related to the new technologies." All branches of the federal government and all provincial and municipal governments were invited to participate in this Task Group. Argentine Republic, Presidential Decree No. 512/2009, http://www.glin.gov/view.action?glinID=218624 (May 7, 2009).

156. DSR art. 11-17.

157. DSR art. 24 and 26. When the DSR was originally enacted, art. 30 mandated a CA to carry insurance. Art. 30 was repealed in 2006. *See* DSA, *supra* n. 91, art. 1 (second citation). Also, the government does not guarantee the quality of service provided by a licensed CA. DSR art. 25.

158. DSR art. 32.

159. DSR art. 22.

160. DSR art. 29.

issuance of certificates to them; if the security of a private key has been compromised, the certificate must be promptly revoked and all parties must be informed.[161] A CA may employ a Registration Authority to perform the clerical procedures relating to the identification of subscribers and the issuance and administration of certificates.[162] Certificates issued by foreign CA's may be recognized in Argentina, providing the foreign CA is in compliance with Argentine law.[163] A CA may revoke a certificate previously issued in ten (10) types of situations.[164]

The chief of the Cabinet of Ministers also appoints auditors to conduct annual audits of CA's.[165] The CA's license may be revoked if any of five (5) grounds are present.[166] A third party may refuse to acknowledge the validity of the certification if its standards are more stringent to than those of a particular CA.[167]

All government departments are mandated to provide E-government services,[168]and the digital signatures must be provided to citizens for free.[169]

V. RECOMMENDATIONS FOR IMPROVEMENT OF ARGENTINE E- COMMERCE LAW

Argentina has made a satisfactory beginning in its E-commerce law. However, it has not gone far enough; the following amendments should be considered.

A. ENACT A COMPREHENSIVE ELECTRONIC TRANSACTIONS LAW

All of the laws pertinent to electronic transactions should be included under the umbrella of the new Electronic Transactions Law ("ETL"). A comprehensive statute will improve the existing law because the various E-commerce laws will be easier for all affected parties to research and to

161. DSR art. 34.
162. DSR art. 35-36. The use of a Registration Authority is exemplary and is recommended for adoption by other nations.
163. DSR art. 28.
164. DSR art. 23.
165. DSR art. 18-21 and 26.
166. DSR art. 27.
167. Art. 34 of the original DSR did not allow a third party to refuse to accept a digitally signed E-document if its validity standards were more stringent than that of the attesting CA. However, art. 34 was amended in 2006 by DSA art. 4. *See* DSA, *supra* n. 91 (second citation).
168. DSR art. 37-46.
169. In the original DSR, free digital signatures were not provided. However, the DSR was amended in order to promote E-government participation by citizens. *See* DSA, *supra* n. 81, art. 2 (second citation).

comprehend. Accordingly, other existing laws pertinent to electronic transactions should be consolidated into the ETL.

The ETL should include the following sections: Introduction; Legal Recognition of Electronic Form and Secure Electronic Documents and Signatures; Legal Presumptions, Admissibility and Evidential Weight of Electronic Evidence in a Court of Law or Administrative Proceeding; Use of Electronic Form to Comply With Requirements of Other Statutes; Regulation of CA's; Duties and Liabilities of CA's; Duties of Subscribers and Relying Third Parties; Electronic Contracts; Consumer Protections in E-Commerce Transactions; Computer Crimes; Computer Criminal and Civil Justice; E-Government; Domain Name Registration; Network Intermediaries; Privacy of Information; and Other Issues.

B. MAKE THE ETL SUPREME IN ALL THINGS ELECTRONIC

If the ETL is in conflict with another law or statute of Argentina, the ETL should prevail. This will improve the existing law because there will be no doubt that the provisions of the ETL are to be adhered to and will override other conflicting laws. This advantage is similar to the supremacy of U.S. federal law over state and local law.

C. ADD: A LIST OF OTHER LAWS AFFECTED BY THE ETL

There should be a list of other statutes and regulations that are modified or affected by the ETL. This provision will improve the existing law because it will specify the impact of the ETL upon other laws. Additionally, there should be a list of the names of all other statutes, currently in force (and the applicable provisions in each), which can be complied with using the electronic form instead of the paper form. This provision will improve the existing law by authorizing use of E-documents in other specified statutes, thereby making compliance with those statutory requirements more convenient and cheaper.

D. DELETE: ALL EXCLUSIONS

The Argentine Digital Signature Law contains several exclusions from coverage. The result is that several types of documents must be in paper form to have legal validity: wills and codicils; [170] family law documents,

170. The aversion to electronic wills is beginning to dissipate. In 2005, the U.S. State of Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature. *See* Chad Michael Ross, Comment, *Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will*, 35 UNIVERSITY OF MEMPHIS LAW REVIEW 603 (2005).

including marriage licenses and divorce decrees; documents in situations involving "very personal events;" documents in situations which are incompatible with the digital form; and whenever the parties have agreed not to use digital documents.[171]

All of the exclusions (except for agreement of the parties) should be eliminated. This would improve the existing law by recognizing the legal validity of electronic documents in all situations, except when the parties have made a contrary agreement. Unlimited utilization of E-documents would result in greater convenience and economy in more types of transactions. This would firmly tell the world that Argentina sees virtually no limits to the utilization of the electronic form and would hasten the adoption of the electronic form by its citizens and residents. Only a few nations have completely eliminated exclusions in their E-commerce statutes,[172] and none of them are in South America.

E. LEGAL VALIDITY OF ELECTRONIC FORM TO COMPLY WITH SEVERAL ADDITIONAL REQUIREMENTS OF OTHER STATUTES

The ETL should state a general presumption that the electronic form may be used to satisfy requirements contained in other statutes, which are prerequisite to incurrence of a legal right. Those requirements include, but are not limited to, the following: the witnessing of a handwritten signature or seal; a paper document's notarization, certification, acknowledgement, verification, attestation, or being made under oath; production of multiple copies of a paper document (where production of one electronic copy is sufficient); communication by registered or certified mail (provided that the electronic message is transmitted thorough the sender's Certification Authority and confirmed by him); and seller's provision of a notice to a consumer in writing. This would improve the existing law by enabling the utilization of E-documents in more situations, thereby making those transactions cheaper and more

171. DSL art. 4.

172. For example, Azerbaijan's statute contains no exclusions from coverage; it states that electronic documents "can be used (applied) in *all activity spheres* where software and technical equipment could be applied to create, use, store, transmit and receive information." Republic of Azerbaijan, ELECTRONIC DOCUMENT LAW, 2003, art. 1(1) (emphasis added), *supra* n. 69. Iran, Montenegro, New Zealand and Tunisia also have no exclusions from coverage. *See* Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN, http://irtp.com/laws/ec/IR%20Iran%20E-Commerce%20Law.pdf (2003); Republic of Montenegro, ELECTRONIC SIGNATURE LAW, www.mipa.cg.yu (2003); Commonwealth of New Zealand, ELECTRONIC TRANSACTIONS ACT, http://www.med.govt.nz/templates/MultipageDocument Page____9779.aspx (2000); and Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, http://www.bakernet.com.org (Aug. 9, 2000).

convenient. For a comprehensive list of such electronic compliance allowances, refer to the New Zealand statute.[173]

F. E-CONTRACT RULES

As mentioned, Argentina should include E-contract rules in its Electronic Transactions Law. Several types of E-contract rules are needed, as follows:

For attribution, refer to South Korea's Electronic Commerce Act.[174] This would improve the existing law by specifying the rules relating to whether the communiqué of a personal agent or a computerized agent may be attributed to a party.

For acknowledgement of receipt, look to Singapore's Electronic Transactions Act.[175] This would improve the existing law by specifying rules relating to whether the receiver of an E-message is required to acknowledge receipt to the sender.

For time and place, use Holland's Electronic Commerce Act.[176] This would improve the existing law by specifying rules to be used in determination of the time and place that an E-communique is assumed to have been sent or received.

For carriage contracts, Colombia's Electronic Trade Law has a commendable paradigm.[177] This would improve the existing law by specifying rules to be employed in E-contracts relating to the delivery of goods.

---

173. *Id.* (fourth citation).

174. Republic of South Korea, Korean Legislation Research Institute ("KLRI"), FRAMEWORK ACT ON ELECTRONIC COMMERCE, *Statutes of the Republic of Korea,* vol. 13, 395-400 (1999). The KLRI is an independent non-profit organization funded by the government of the Republic of South Korea. The KLRI's charge is to translate all of the Korean federal statutes into English. They do an admirable job of this, and the *Statutes'* twenty volumes, in loose-leaf form, are continually updated. This is one of the Korean government's globalization thrusts. Of course, the "official" statutes are the ones in Korean Language as originally enacted. However, given that the KLRI's work is financed by the Korean government, the English-Language versions of the statutes used in research for this article could be described as "*quasi*-official." *See* Stephen E. Blythe, *supra* n. 86.

175. UNCITRAL, *supra* n. 64, s 14 (first citation).

176. Kingdom of the Netherlands, ACT ON INFORMATION SOCIETY SERVICES (June 30, 2004), Art. 11. *See* Stephen E. Blythe, *supra* n. 65 (first citation).

177. ETL, *supra* n. 73.

For automated contracts, the U.S. Uniform Electronic Transactions Act contains a good model.[178] This would improve the existing law by specifying rules to be used whenever a computer has been programmed to automatically enter into a contract with a person or a person represented by another programmed computer.

G. CONSUMER PROTECTIONS FOR E-BUYERS

Argentina needs to enact a general consumer protection statute applicable to all internet consumers. This would improve the existing law and would foster the growth of E-commerce by instilling confidence in E-buyers that the ETL will protect them from fraudulent or unfair trade practices of E-sellers.

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.[179]

H. I.T. COURTS FOR E-COMMERCE DISPUTES

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. This would improve the existing law by ensuring that the adjudicating body has the expertise necessary to render a fair and knowledgeable decision in E-contract cases.

---

178. United States of America, National Conference of Commissioners on Uniform State Laws, *supra* n. 59. *See* Stephen E. Blythe, *supra* n. 60 (both citations).

179. Republic of Tunisia, *supra* n. 88. One of the few nations that may offer better consumer protections is Korea. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act. *See* Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions ("CPA"), STATUTES OF THE REPUBLIC OF KOREA, Vol. 13, pp. 481 to 485-30. Originally enacted by Law No. 6687 (30 March 2002), and amended by Act Nos. 7315 and 7344 of 31 December 2004 and 27 January 2005, respectively. The CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of 31 March 2005; those amendments became effective on 1 April 2006. For an analysis of the CPA, *see* Stephen E. Blythe, *supra* n. 86. Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-commerce transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Stephen E. Blythe, *supra* n. 79.

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.[180]

I. LONG-ARM JURISDICTION AGAINST FOREIGN E-COMMERCE PARTIES

Because so many of the E-commerce transactions incurred by the residents of Argentina will be with parties outside the borders of Argentina, 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 Argentina. This will improve the existing law by requiring a foreign party to come to Argentina to adjudicate a dispute relating to an E-contract made with an Argentine citizen or resident. Accordingly, the Argentine party would incur the relative convenience and economy of adjudicating the dispute in his home country.

Minimum contacts will exist if a cyber-seller outside of the country makes a sale to a person in Argentina. In that situation, Argentine laws 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 Argentina. The foreign party should not be allowed to evade the jurisdiction of the Argentine courts merely because he is not physically present in the country. After all, E-commerce is an inherently international and multi-jurisdictional phenomenon. The Kingdom of Tonga can be used as a model.[181]

J. NATIONAL ID CARD WITH DIGITAL SIGNATURE

Argentina should adopt a National ID Card. This would improve the existing law because: (1) the Argentine government would develop an electronic database of information relating to its citizens and residents, resulting in greater national security and in cost savings; and (2)

180. Federal Democratic Republic of Nepal, *supra* n. 55.

181. The Republic of Tonga explicitly states its claim of long-arm jurisdiction over foreign E-commerce parties. *See* Stephen E. Blythe, Note 88 *supra* n. 90.

Argentine citizens and residents would incur more convenience because the ID Card could be used to access E-government services, and a computer chip in the ID Card could be used as a personal digital signature.

The National ID Card would contain several types of personal information, including voter registration.[182] Application and other information pertinent to the National ID Card should be made available at the Government Portal. Only a handful of other jurisdictions have adopted an ID card; they include Belgium[183] and Hong Kong.[184] In those jurisdictions, the ID Card's computer chip can serve as the digital signature of the cardholder.[185]

K. ARGENTINA'S POST OFFICE TO BECOME A LICENSED CERTIFICATION AUTHORITY

Designation of the Argentine Post Office as a licensed CA would improve the existing law by promoting the utilization of E-signatures among the general public and would make E-signatures cheaper and more accessible. For a model, look to the Belgian Post Office, which has implemented a promotional campaign to educate the general public about E-signatures and their availability through the Post Office.[186]

---

182. Privacy International, PHR2006: THE HASHEMITE KINGDOM OF JORDAN, 2, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559523 (Dec. 18, 2007).

183. By 2010, Belgium will have issued an electronic ID card to each of its 9 million inhabitants, becoming the first European nation to carry out this achievement. Each resident will pay approximately EU 10 for his card. These cards contain two E-signatures; one will be used for identification of the holder, and the other will be used to sign E-documents. Already, the electronic ID card is being used for: access to the Belgian government website and its E-government services; signing of legal documents in digital form (e.g., tax declaration, VAT declaration, and social security affirmations); access to community container parks; parking tickets; signing of registered mail; signing of Flemish Parliament Decrees; requests for official documents and access to National Register records; and access to the E-library service. Additionally, Dell, HP and Siemens computers are now able to read the Belgian ID card and to process its E-signature data. Interdisciplinary Centre for Law & Information Technology, THE LEGAL AND MARKET ASPECTS OF ELECTRONIC SIGNATURES, 177-178, http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf (2003).

184. Rina C.Y. Chung, *supra* n. 22. For information pertinent to the Hong Kong I.D. card, refer to the Hong Kong Government Portal, http://www.smartid.gov.hk/. The list of other nations having adopted national ID cards includes: Austria, Bahrain, Belgium, Hong Kong, Israel, Italy, Jordan, Spain and the United Arab Emirates.

185. Rina C.Y. Chung, *supra* n. 22.

186. Kingdom of Belgium, LEGAL FRAMEWORK FOR ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES ("ESA"), (July 9, 2001). This statute was supplemented by the ROYAL DECREE ORGANIZING THE SUPERVISION AND ACCREDITATION OF CERTIFICATION SERVICE PROVIDERS ISSUING QUALIFIED CERTIFICATES, (Dec. 6, 2002).

L. SEVERAL NEW COMPUTER CRIMES

The list of computer crimes needs to be expanded. This would improve the existing law because it would reduce the likelihood of several types of fraudulent or malicious acts relating to computer systems.

The following computer crimes, with appropriate penalties, should be recognized: (a) Unauthorized Tampering with Computer Information; (b) Unauthorized Use of a Computer Service; (c) Unauthorized Interference in the Operation of a Computer; (d) Unauthorized Dissemination of Computer Access Codes or Passwords; and (e) Injection of a Virus into a Computer. The Singapore Computer Misuse Act can be used as a model.[187]

M. ADOPT A THIRD GENERATION E-SIGNATURE LAW

Argentina should join the third generation of E-signature laws. The Digital

Signature Law should be re-named the Electronic Signature Law. All types of E-signatures should be recognized, although higher status in terms of presumed security should be given to the digital signature. This would improve the existing law because it would facilitate the creation, legal recognition and enforcement of E-contracts that have been consummated using an E-signature that is not a digital signature.

VI. CONCLUSIONS

The Argentine statutes need to be refined as follows:

The ETL should be comprehensive. All laws relating to E-commerce should be consolidated into the ETL in order to promote better understanding of the interrelationship of those laws and to improve the convenience of research.

The ETL should be supreme in all things electronic. Just as the Federal Supremacy Clause grants U.S. federal law supremacy over state and local laws, the ETL should be declared to be supreme over all over other Argentine laws relating to E-commerce.

---

187. Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A (August 30, 1993). *See* Stephen E. Blythe, *supra* n. 64 (second citation).

A list of other laws affected by the ETL should be included. For example, if the ETL were to include a provision that allowed the payment of income taxes electronically, the name and citation of the income tax law should be listed in the ETL.

All exclusions from coverage should be eliminated. This would expand the number of types of transactions that can be consummated electronically, resulting in greater efficiency and convenience for the general public.

The ETL should recognize the legal validity of the electronic form in order to comply with several additional requirements of other statutes. For example, if another statute mandates a notary public's attestation of a signature on a paper document, that statute should also recognize the legal validity of a notary public's attestation of an E-signature on an E-document.

E-contract rules relating to attribution, acknowledgement of receipt, time/place of transmission/receipt, automated contracts and electronic carriage contracts should be added. These rules would govern: whether a received E-message should be attributed to a specific person; whether it is required for the receiver of an E-message to inform the sender of the E-message that it has been received; the time and place it may be assumed that an E-message has been transmitted or received; the consummation of contracts between two programmed computers or between a programmed computer and a person; and E-contracts relating to the delivery of goods.

Consumer protections for E-buyers should be added. These provisions will help to ensure that E-buyers are kept informed by the seller, that they are given a reasonable opportunity to opt out of an E-commerce purchase after it has been consummated, and these provisions will specify their legal rights whenever the seller engages in fraudulent or unfair practices.

I.T. Courts should be created for resolution of E-commerce disputes. A panel of three experts—a computer expert, an E-commerce attorney, and an E-business expert—should be used to adjudicate those disputes because an ordinary judge may not possess the requisite technical and business expertise.

"Long-arm" jurisdiction over foreign E-commerce parties should be asserted in the ETL. Argentine citizens and residents should be able to

adjudicate their E-commerce disputes in Argentine I.T. Courts instead of having to go to a foreign court.

The Argentine Post Office should be a licensed Certification Authority. This would enable every Argentine citizen and resident to go to the local post office to apply for the issuance of a certificate relating to his E-signature. This would: reduce the cost of a certificate; increase the number of locations in which citizens and residents can find a CA, resulting in more convenience; and significantly increase the utilization of E-signatures among the general public.

Registration Agents should be authorized to assist Certification Authorities. These agents should be allowed to perform a number of clerical duties on behalf of CA's, process applications for certificates, and issue ordinary types of certificates. If Registration Agents are used, the total cost of CA services should be reduced.

Argentina should begin issuing National ID Cards to all citizens and residents. This would increase national security and would establish a convenient database of information relating to its citizens and residents. If a digital signature is added to the ID Card, this would increase the utilization of E-signatures among the population.

Several new computer crimes should be added to reduce the likelihood of computer fraud, identity theft, and unfair practices.

The ETL should adopt a third-generation E-signature law by recognizing the legal validity of all types of E-signatures. This will make it easier to consummate an E-contract between parties which use different types of E-signatures. Furthermore, this will make the Argentine ETL more comparable with the majority of other nations.