ON TOP OF THE WORLD AND WIRED: A CRITIQUE OF NEPAL'S E-COMMERCE LAW

Stephen E. Blythe*

Cite as: 8 J. HIGH TECH. L. 1 (2008)

Editor's Note: Portions of this article have been previously published. Sections III: Electronic Signatures and Section IV: Three Generation of Electronic Signature Law were published in A Critique of India's Information Technology Act and Recommendations for Improvement by Stephen E. Blythe, 34 Syracuse J. Int'l L. & Com. 1 (2006).

I. Objectives of the Article

The objectives of this article are to: (1) describe the economic and political problems currently facing Nepal; (2) explain the positive role that e-commerce could have in the economic development of the country; (3) explain the role of electronic signatures, cryptology, public key infrastructure, and certification authorities; (4) describe the three generations of electronic signature law and how Nepal fits into that categorization; (5) analyze and critique Nepal's Electronic Transactions Ordinance ("ETO"); and (6) make recommendations for improvement of the ETO. The author's commentaries and recommendations pertinent to the ETO are in **bold type**.

II. Welcome to the Kingdom of Nepal

A. A Tourist Mecca

If anyone wants to become a certified world traveler, the Kingdom of Nepal is a "Must See" destination. This hiker's paradise, perched on top of the world and sandwiched between the two most populous nations on Earth is blessed with beautiful scenery and breathtaking mountains. Each year Nepal attracts hordes of tourists making tourism one of Nepal's most important industries.[1]

* Professor of Law and Accounting, New York Institute of Technology, CERT Technology Park, Abu Dhabi, United Arab Emirates. Ph.D. Candidate (Int'l

B. Economic Underdevelopment

However, despite its natural splendor, Nepal continues to be one of the poorest nations in the world.[2] The economic statistics paint a grim picture. Gross Domestic Product ("GDP") per capita in 2006 was estimated to be only U.S. $1500.[3] Thirty-one percent of the people have annual incomes below the poverty line.[4] The annual per capita income in Nepal is U.S. $290.[5] Forty-two percent of the Nepalese are unemployed.[6] Seventy-six percent of the employed population works in agriculture[7], which accounts for 38 percent of the nation's GDP.[8] Nationwide, only 31 percent of the citizens of Nepal have electricity[9], in spite of the fact that Nepal has large potential for the exportation of

E-commerce Law), The University of Hong Kong (China); Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law) University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. He practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with Cheek, Cheek & Cheek, Attorneys at Law (insurance-defense litigation) in Oklahoma City, and was a management consultant for the city government of Haikou, China. Additionally, he has taught law, accounting, management, economics and international business at thirteen universities located in the United States, Africa and the Middle East.

1. Admittedly, however, Nepal's tourist activity, especially from the U.S., was somewhat adversely affected by the events of September 11, 2001. Additionally, tourism has been hurt by the growing political unrest in the country caused by the Maoist insurgency. *See infra* Part II.C.

2. U.S. Central Intelligence Agency ("CIA"), THE WORLD FACTBOOK: NEPAL, ECONOMY-OVERVIEW 2007, *archived at* http://www.webcitation.org/5T0Z8R74W.

3. CIA, *supra* note 2, at Economy; GDP per capita (PPP). This did show an improvement, however, from 2003, when GDP per capita was estimated to have been only U.S. $1310. *See* United Nations Capital Development Fund, Countries and Regions, Nepal, *archived at* http://www.webcitation.org/5TNR3BoxG.

4. Based on Fiscal year 2003/2004. CIA, THE WORLD FACTBOOK, FIELD LISTING – POPULATION BELOW POVERTY LINE, NEPAL, *archived at* http://www.webcitation.org/5TNQjp5q4.

5. BBC News, Country Profile: Nepal, *archived at* http://www.webcitation.org/5TNTz9gO9.

6. CIA, *supra* note 2.

7. CIA, *supra*, note 2. This is based on a 2004 estimate. Nepal's agricultural products include rice, corn, wheat, sugarcane, jute and root crops. *Id*. Additionally, Nepal's most important exported goods are carpets, pashmina products, clothing, leather goods, handicrafts, jute goods and grain. Tika R. Kandel, *E-commerce: To Enhance SMEs' Performance*, Worldwide Nepalese Students' Organization Newsletter, *archived at* http://www.webcitation.org/5TkNskjWx.

8. CIA, *supra* note 2.

9. United Nations Development Programme, NEPAL HUMAN DEVELOPMENT REPORT 2004 40, *archived at* http://www.webcitation.org/5TP0C0JCA.

hydropower.[10] The life expectancy of a Nepalese is just over 60 years and 51 percent of the people aged 15 and above cannot read or write.[11] The country is very dependent on foreign aid for its survival, with the international community providing substantial economic aid.[12] Furthermore, Nepal's economic prospects remain dim because of the "small size of the economy, its technological backwardness, its remoteness, its landlocked geographic location, its civil strife, and its susceptibility to natural disaster."[13]

C. Political Instability

Adding to Nepal's economic woes is the ever-growing problem of political instability. Nepal's government is a parliamentary democracy and a constitutional monarchy, but this government is being threatened.[14] A Maoist insurgency has been trying to overthrow the government since 1996, and the insurgency has recently been growing stronger.[15] Negotiations achieved a cease-fire between the Maoists and the government in August 2003, but subsequently broke down, and the insurgency reactivated.[16]

On June 1, 2001, the monarchy was further shaken from within by a tragic and unexpected event.[17] The Crown Prince of Nepal inexplicably shot and killed his father, the King of Nepal, and several other members of the royal family before turning the weapon on himself.[18] Before he died, however, the Crown Prince lay in a coma for three days, during which he became King.[19] Upon his death on June 4, 2001, the crown passed to the Crown Prince's uncle, the current monarch, King Gyanendra.[20]

10. CIA, *supra* note 2.
11. CIA, *supra* note 2.
12. CIA, *supra* note 2 Nepal received $533 million in aid for FY 04/05. *Id.*
13. CIA, *supra* note 2.
14. CIA, *supra* note 2.
15. CIA, *supra* note 2.
16. CIA, *supra* note 2.
17. CIA, *supra* note 2.
18. Barbara Crosette, *Royal Family of Nepal Is Shot Dead in Palace*, N.Y. TIMES, June 2, 2001, at A1.
19. Barry Bearak, *Royal Bloodbath Suspect Is Nepal's King, for Now*, N.Y. TIMES, June 3, 2001, at 1.
20. CIA, *supra* note 2. By sheer coincidence, the author arrived as a tourist in Nepal's capital city, Kathmandu, only a few hours after the Crown Prince had committed the murders. The city was in a state of shock and despair. The royal corpses were publicly cremated the day following the murder, and the event was televised. The next day, both pro-monarchy groups and anti-monarchy groups began to stage large demonstrations. To prevent violence, the government invoked a temporary ban on public gatherings, citizens were confined to their homes and

In October 2002, King Gyanendra dismissed the Prime Minister and his cabinet for "incompetence" after they had dissolved the parliament and was subsequently unable to hold elections due to the growing insurgency.[21] In June 2004, the King reinstated the most recently elected former Prime Minister who formed a four-party coalition government, but he did not reconvene the parliament.[22] The King however grew dissatisfied with the Prime Minister's inability to deal with the Maoist insurgency and with its alleged corruption.[23] In February 2005, the King declared a state of emergency. He dissolved the Prime Minister's government, imprisoned the leaders of the four political parties, and assumed total power.[24]

In May 2005, the King declared an end to the state of emergency and released the political party leaders.[25] However, the King retained absolute power over the country.[26] In early 2006, the Maoists and seven opposing political parties instigated three weeks of widespread protests to voice their dissatisfaction with the King's stranglehold on power.[27] At first, the King attempted to control the protestors with strong-arm tactics, using his police force who killed a number of Nepalese citizens.[28] Eventually, however, the King relented allowing the parliament to reconvene on April 28, 2006.[29] These events set the stage for a political deal in December of 2007 between Nepal's government and the Maoist former rebels which will end the Nepalese monarchy in 2008.[30]

D. Room For Hope

Notwithstanding these dramatic economic and political difficulties, there is room for hope in Nepal. Two significant sources of foreign exchange triggered the interests of foreign investors.[31] After facing

tourists were confined to their hotels. No private cars or taxis were allowed to be driven, so the author had to request transportation from the American Embassy to the Kathmandu Airport, which was provided.

21. CIA, *supra* note 2.
22. CIA, *supra* note 2.
23. CIA, *supra* note 2.
24. CIA, *supra* note 2.
25. CIA, *supra* note 2.
26. CIA, *supra* note 2.
27. CIA, *supra* note 2.
28. Microsoft® Encarta® Online Encyclopedia 2007, NEPAL [hereinafter NEPAL], *archived at* http://www.webcitation.org/5Th2d9Ma7.
29. CIA, *supra* note 2.
30. *Nepal to End Its Monarchy in a Deal With Ex-Rebels*, N.Y. TIMES, December 24, 2007, at A8.
31. CIA, *supra* note 2.

some difficulties the past few years, tourism seems to be on the rebound and is expected to grow.[32] Furthermore, Nepal is committed to the development of its hydroelectric power industry.[33]

There is another point of light, which may offer potential improvement for Nepal's future, e-commerce.[34] In 2000, seeing this potential Nepal's Ministry of Science & Technology coordinated with the United Nations Conference on Trade and Development (UNCTAD)[35] sponsoring a conference held in Kathmandu.[36] The topic under consideration was "Electronic Commerce & Development for the Least Developed Countries (LDCs)." Representatives from forty other LDC nations attended the conference to learn how to thrive in the world of e-commerce.[37]

Since 2000, a number of websites have emerged in Nepal for the purpose of marketing Nepalese goods on an global scale.[38] However, an important piece of the e-commerce roadmap was missing - a comprehensive e-commerce law. That missing piece was added in 2004,

32. Michael Verikios, *Steady Growth in Tourist Arrival Continues for Nepal*, TRAVEL DAILY NEWS, Nov. 08, 2007, *archived at* http://webcitation.org/5Th3v1Twv.

33. NEPAL, *supra* note 28.

34. For an article pertaining to identification of projects that might lead to growth of e-commerce in Nepal, *see* Penjor Ngudup, *E-commerce in Nepal: A Case Study of an Underdeveloped Country*, 2:3/4 INT'l J. MGMT. & ENTER. DEV. 306 (2005). For an older article with a similar theme, *see* Larry Press, Seymour Goodman, Tim Kelly & Michael Minges, *Electronic Commerce in Nepal*, E-OIT: ON THE INTERNET, Mar./Apr. 2001, *archived at* http://www.webcitation.org/5T0bjmFTP.

35. *See generally* United Nations Conference on Trade and Development, *archived at* http://www.webcitation.org/5WJwQwHFa.

36. *See* Posting of Irfan Khan , KhanIA@super.net.pk, to s-asia-it@apnic.net (June 12, 2000), *archived at* http://www.webcitation.org/5V7TEH35P.

37. *See generally* United Nations Conference on Trade and Development [UNCTD], ICT and e-Business Branch, Roundtable on Electronic Commerce and Development for the Least Developed Countries (LDCs), *archived at* http://www.webcitation.org/5TQlaIXxb.

38. Here are a few examples of Nepalese websites: (1) Muncha House, one of the oldest department stores in Kathmandu, sells online at http://www.muncha.com, *archived at* http://www.webcitation.org/5T2D66F4m; (2) one of many Nepalese jewelry websites is at http://www.wholesalenepal.com, *archived at* http://www.webcitation.org/5T2DB5ERB; (3) B2B is emphasized at the National Business-to-Business E-commerce Market Place "Nepali e-Haat Bazaar", *archived at* http://www.webcitation.org/5T2DEghGl. The latter is supposedly a "single electronic gateway to promote the market linkages within the country and with the international markets." Kandel, *supra* note 7, at 3. Other business firms have established successful commercial websites at: NetforNepal.com, *archived at* http://www.webcitation.org/5T2DMHIoy; Shopnbds.com, *archived at* http://www.webcitation.org/5T2DPYdQw; thamel.com, *archived at* http://www.webcitation.org/5Tn15ph9J.

providing the centerpiece of this article's analysis.[39]

One of the most important parts of Nepal's e-commerce law concerns one type of electronic signature - the digital signature. In order to lay the foundation for a discussion of the pertinent legal issues, it is appropriate at this point to consider the basic aspects of electronic signatures in general and of digital signatures in particular.

II. Electronic Signatures

Contract law worldwide traditionally required the parties to affix their signatures to a document.[40] 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,"[41] 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."[42] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a personal identification number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[43]

A well-known U.S. consumer group has stated: "[G]iven the current state of authentication technology, it's much easier to forge or steal an e-

39. Ram Chandra Subedi, *Cyber Law: A Challenge to Legal System*, HIMALAYAN TIMES, 2004-05, *archived at* http://www.webcitation.org/5TQlqm3yy.

40. *See, e.g.*, U.C.C. §§ 2-201, 2-209 (1998).

41. Thomas J. Smedinghoff, *Electronic Contracts and Digital Signatures: An Overview of Law and Legislation*, *in* PATENTS, COPYRIGHTS, TRADEMARKS & LITERARY PROPERTY COURSE HANDBOOK, 127, 162 (Prac. Law Inst. 1999).

42. Council Directive 1999/93, 2000 O.J. (L13/14) (EU), *archived at* http://www.webcitation.org/5TQmwf6Pc. Nepal defines electronic form as "a form of information transmitted, received or stored by generating the same through the means of magnetic, optical, computer memory or similar other devices" and an "electronic record" is defined as "data, record, image, or sound transmitted, received or stored in an electronic form by generating the same through any means". *See* Electronic Transactions Ordinance, 34 NEPAL GAZETTE 60, No.32 OF THE YEAR 2061 B.S. (2004 A.D.), § 2(v)-(w) [hereinafter ETO]. The original version, in Nepalese Language, is available at the website of the Nepal Telecommunications Authority, *archived at* http://www.webcitation.org/5V7Y4QvhM. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the NEPAL GAZETTE on March 18, 2005, *archived at* http://www.webcitation.org/5T2E4pgwf.

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

signature than a written one."[44] This statement seems to assume that all e-signatures offer an equal degree of security. However, some electronic signatures offer more security than others.[45] It is prudent for e-commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

A. Online Contracts: Four Levels of Security

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

a. The first level is achieved when a party accepts an offer by merely clicking an "I Agree" button on a computer screen.[46]

b. The second level of security is achieved when confidential information is shared between the two contracting parties. For example, the use of a password or the entry of a credit card number to verify a customer's intention to purchase goods or services.[47]

c. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and are extremely difficult for a would-be cyber thief to replicate.[48] Examples include a voice pattern, face recognition, a scan of an individual's retina or iris, a digital reproduction of a fingerprint[49], or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison with a person purporting to have the same identity.[50] For example, if a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet

44. Michael Dessent, *Browse-Wraps, Click-Wraps and Cyberlaw: Our Shrinking (Wrap) World*, 25 T. JEFFERSON L. REV. 1, 6-7 (2002).

45. *See* discussion *infra* Part III.A-D.

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

47. *Id.*

48. *Biometrics 101, What Are Biometrics?*, BIOMETRICS TASK FORCE, DEPARTMENT OF THE ARMY, *archived at* http://www.webcitation.org/5Tn28NKxl.

49. In the highly successful Hong Kong Identity Card, 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-PAC. L. & POL'Y J. 519, 541 (2003).

50. *See* Stern, *supra* note 46, at 395-96; *The Legality of Electronic Signatures Using Cyber-Sign is Well Established*, CYBER SIGN, *archived at* http://www.webcitation.org/5V7Z6kERJ.

motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter.[51] Biometrics, despite its potential utility as a form of electronic signature, has at least two drawbacks in comparison with the more secure 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;"[52] 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.[53] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[54] Many also recommend the use of both methods; this was the course taken by Hong Kong's government in designing its identity card.[55]

d. The digital signature[56] 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, however, is not the case as the digital signature refers to the entire

51. *See* Stern, *supra* note 46, at 395-96; Cyber-Sign, *supra* note 51.

52. 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, 256-57 (2002).

53. *Id.* at 257.

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

55. *See* Chung, *supra* note 50.

56. Nepal defines a digital signature as "a signature made in any electronic form to be included in the transformation of electronic record by a person having a non-transformed initial electronic record and the public key of signatory by using a type of asymmetric crypto system that may clear ascertain the following matters: (1) Whether or not transformation of electronic record was created by using a type of private key keeping a logical consistency with the public key of signatory; and (2) Whether or not the initial electronic record has been changed after the transformation of electronic record." *See* ETO *supra*, note 43, § 2(o).

> document.[57] It is "the sequence of bits that is created by running an electronic message through a one-way hash function to create a unique digest, or 'fingerprint', of the message and then using public key encryption to encrypt the resulting message digest with the sender's private key."[58] 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.[59]

B. Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure (PKI).[60] PKI consists of four steps:

a. The first step is creating a public-private key pair. The sender keeps the private key in confidence[61], but the public key is available online.[62]

b. Next, the sender digitally "signs" the message by creating a unique digest of the message and encrypting it. A "hash value", a sequence of 160 bits that is a digest of the document's contents, is created by applying a "hash function", a standard mathematical function, to the contents of the electronic document. The hash function is then encrypted, or

57. 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." Stephen Blythe, *Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-commerce in the World's "Most Wired" City*, 7 N.C. J. L. & TECH. 1, 6 (2005).

58. Hossein Bidgoli, HANDBOOK OF INFORMATION SECURITY: THREATS, VULNERABILITIES, PREVENTION, DETECTION, AND MANAGEMENT, 397 (Wiley 2006).

59. 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).

60. Susanna Frederick Fischer, *California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, 7 B.U. J. SCI. & TECH. L. 229, 233 (2001).

61. ABA PKI Assessment Guidelines, V 0.30 at 301 (Public Draft for Comment No. 25, 2001), a*rchived at* http://www.webcitation.org/5T2DsmuFh.

62. *Id.* at 305.

scrambled, by the signatory using his private key. Asymmetric encryption provides one of the highest, if not *the* highest, degrees of security in electronic transactions. The encrypted hash function is the "digital signature" for the document.[63]

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

d. Lastly, the recipient decrypts the digital signature by using the sender's public key. If decryption is possible the recipient knows the message is authentic, i.e., that it came from the purported sender. Finally, the recipient creates a second message digest of the communication and compares it to the decrypted message digest.[64] If they match, the recipient knows the message has not been altered.[65]

C. 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.[66] Furthermore, the encryption[67] of the hash value with the signatory's private key "links the uniquely digital signature to the signatory, i.e., the owner of the private key."[68] While a handwritten signature is only "signatory-specific," a digital signature is both "signatory-specific" and "document-specific."[69]

The digital signature is the only form of electronic signature which satisfies all three of the United Nations Commission on International Trade Law ("UNCITRAL") security evaluation factors. UNCITRAL indicates that an electronic signature should: (1) authorize; (2) approve;

63. Pun, *supra* note 53, at 249.

64. American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, Section of Science & Technology, Information Security Committee, Electronic Commerce & Information Technology Division, 1996 A.B.A. SEC. SCI. & TECH. at 9, *archived at* http://www.webcitation.org/5Tn3gfQXD.

65. Jochen Zaremba, *International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers*, 18 CONN. J. INT'L. L. 479, 512 (2003).

66. Pun, *supra* note 53, at 249.

67. Nepal defines an "Asymmetric Crypto System" as "a system that creates a secured key-pair consisting of a private key creating a digital signature and a public key to verify the digital signature." *See* ETO, *supra* note 42, § 2(a).

68. *See* Pun, *supra* note 53, at 250. Nepal defines "Private Key" as "the one (of a key-pair) used to create a digital signature." *See* ETO *supra* note 43, § 2(m).

69. *See* Pun, *supra* note 53, at 250.

and (3) protect against fraud.[70] 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 electronic document's hash value 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.[71]

D. Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. First, since the private key is rather difficult to memorize, it is often stored in a computer. Computers not kept in a secure location may compromise the contents of the private key. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. It should be noted, however, that this weakness of the digital signature is also common to most other forms of electronic signatures. Passwords and personal identification numbers ("PIN") face similar security problems. Therefore, good security policies and procedures can minimize this disadvantage.[72]

The other disadvantage of the digital signature pertains to the certificate, which must be issued by a Certifying Authority ("CA").[73] 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.[74] Since the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

E. The Critical Role of the Certifying Authority

In order for PKI to realize its potential, it is crucial that the user be

70. *See* UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, U.N. Comm'n on Int'l Trade Law, G.A. Res. 51/162, at 336, U.N. GAOR, 51st Sess., U.N. Doc. A/Res/51/162 (1996), *archived at* http://www.webcitation.org/5WqLYKmij. *See also* Pun, *supra* note 53, at 243-244.

71. *See* Pun, *supra* note 53, at 252. Nepal defines Public Key as the one (of a key-pair) "used to verify a digital signature." *See* ETO, *supra* note 42, § 2(x).

72. Pun, *supra* note 52, at 253.

73. *See infra* Part III.E.

74. Pun, *supra* note 52, at 253.

able to ensure the authenticity of the public key (available online) used to verify the digital signature. If A (the sender) and B (the receiver) are attempting to consummate an online transaction, B needs an independent confirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that an imposter could have sent B the public key, contending that it belongs to A, when in fact it does not. Accordingly, a reliable third party, the Certifying Authority[75], must be available to register the public keys of the parties to guarantee the accuracy in identification.[76]

The most important job of the CA is to issue a certificate[77], which confirms basic facts about the subscriber[78], the subject of the digital certificate. The certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties: the name and address of the CA that issued the certificate, the name, address and other attributes of the subscriber, the subscriber's public key, and the digital signature of the CA.[79] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[80]

When 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 issued, the CA issues a private key to its new subscriber that corresponds to the public key. This is done, however, without disclosing the specifics of the private key.[81] The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered. Ordinarily, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be

75. Nepal defines the Certifying Authority as a person who "has obtained a license to issue a Digital Signature Certificate under Sub-section (3) of Section 18." ETO, *supra* note 42, § 2(t).

76. Tara C. Hogan, Note, *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).

77. The certificate's purpose is to verify the authenticity of the digital signature and the electronic documents to which the digital signature is affixed. Nepal defines a "certificate" as "a Digital Signature Certificate issued by the Certifying Authority…" ETO, *supra* note 42, § 2(r).

78. Nepal defines a "subscriber" as "a person who has obtained a certificate under sub-section (3) of Section 31." ETO, *supra* note 42, § 2(i). A certificate may only be issued by a Certifying Authority. *Id.* § 30.

79. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 58 (1996) (detailing elements of a certificate).

80. Hogan, *supra* note 76, at 425-26.

81. *See* Smedinghoff, *supra* note 42, at 149.

issued.[82]

In order to indicate the authenticity of the digital certificate, the CA will sign it with his digital signature.[83] Typically, the public key corresponding to the subscriber's private key will be filed in the CA's online repository, which is accessible to the general public and to third parties who have need of communication with the subscriber.[84] 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.[85] This is an important 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 given private key.[86]

Fairly apportioning the liability for risk of computer fraud between the CA and the subscriber represents one of the recurring problems for digital signature lawmakers.[87] Nations around the world have arrived at different conclusions regarding this apportionment. The problem is compounded if each CA is required to modify its practices every time it issues a certificate pertaining to a transaction affecting another jurisdiction which happens to have dissimilar digital signature laws.[88]

A certificate is only as reputable as the CA that issues it. If the CA is unreliable and untrustworthy, the certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and judgment that the subscriber's identification is accurate.[89]

IV. Three Generations of Electronic Signature Law

82. *Id.* at 150.
83. *See* Hogan, *supra* note 76, at 425-26.
84. *See* Hogan, *supra* note 77, at 426.
85. *See* Hogan, *supra* note 77, at 426-27.
86. *See* Hogan, *supra* note 77, at 426.
87. Michael J. Osty & Michael J. Pulcania, *The Liability of Certification Authorities to Relying Third Parties*, 17 J. MARSHALL J. COMPUTER & INFO. L. 961, 969 (1999).
88. Andrew B. Berman, *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); *see also* Alana Maurushat, *Multi-Lateral Recognition of PKI Certification Authorities in the Asia Region: Transborder Data Flow and Information Privacy Issues*, 35 HONG KONG L.J. 569 (2005) (arguing multi-lateral recognition of CA's among China, Hong Kong and Singapore should not occur until their PKI legislation has been harmonized and each provides sufficient privacy protections for personal data).
89. David Hallerman, *Will Banks Become E-Commerce Authorities?* 12 BANK TECH. NEWS, June 1, 1999.

A. The First Wave: Technological Exclusivity

In 1995, Utah became the first jurisdiction in the world to enact an electronic signature law.[90] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[91] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions.[92] Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature include Germany, Italy, Malaysia, Russia[93], Nepal[94], and India.[95]

Unfortunately, these jurisdictions' choice of "technological-exclusivity" is burdensome and overly restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's disadvantages: more expense and complication, less convenience and adaptability to technologies used in other nations, or even by other persons within the same country.[96]

B. The Second Wave: Technological Neutrality

Jurisdictions in the Second Wave overcompensated. They did the complete reverse of the First Wave and did not include any technological restrictions whatsoever in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the other. In other words, they are "technologically neutral." Permissive

90. UTAH CODE ANN. § 46-3-101 (West 1999).
91. *Id.*
92. *Digital Signatures*, WINDOWSECURITY.COM, *archived at* http://www.webcitation.org/5VuQo80YU.
93. Fischer, *supra* note 61, at 234-37.
94. ETO, *supra* note 43.
95. *See* Stephen E. Blythe, *A Critique of India's Information Technology Act and Recommendations for Improvement*, 34 SYRACUSE J. INT'L L. & COM. 1, 14-15 (2006).
96. 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).

jurisdictions provide legal recognition for many types of electronic signatures and do not grant a monopoly to any one. Examples of permissive jurisdictions include the majority of states in the United States, the United Kingdom[97], Canada, Australia, and New Zealand.[98]

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 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 provided by the digital signature.

C. The Third Wave: A Hybrid

Singapore was in the vanguard of the Third Wave. In 1998, this country adopted a 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.[99] In terms of relative degree of technological neutrality, Singapore adopted a "hybrid" model, a preference for the digital signature in terms of greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures. Singapore did not want to become "hamstrung" by tying itself to a one form of technology. The Singapore legislators realized that technology is continually evolving and that it would be unwise to require one form of technology to the exclusion of others. The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[100]

97. For concise coverage of American and British law, *see* Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce With Enhanced Security*, 11 RICH. J.L. & TECH. 6 (2005).

98. *See* Fischer, *supra* note 61, at 234-37.

99. G.A. Res. 51/162, U.N. Doc. A/51/49 (Dec. 16, 1996), *archived at* http://www.webcitation.org/5WqLYKmij; *see also* Blythe, *Digital*, *supra* note 97, at 46.

100. Electronic Transactions Act 25 of 1998, ch. 88, (1998) (Sing.), *archived at* http://www.webcitation.org/5VuDl1BFP. [hereinafter Singapore Electronic Transactions Act] Although granting legal recognition to most types of electronic signatures, the Singapore statute implicitly makes a strong suggestion to users—in two ways—that they should use the digital signature because it is more reliable and more secure than the other types of electronic signatures: (1) digital signatures are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carry a legal

Since 1998, the moderate position adopted by Singapore has become the progressive trend in international electronic signature law. This approach is also employed in the European Union[101], Japan[102], Vanuatu[103], Taiwan[104], Tunisia[105], Lithuania[106], Iran[107], South Korea[108], Barbados[109], Hong Kong[110], Bermuda[111], Pakistan[112], Dubai[113], Azerbaijan[114], and most recently, China.[115]

presumption of reliability and security—these presumptions are not given to other forms of electronic signatures; and (2) although all forms of electronic signatures are allowed to be used in Singapore, its electronic signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the of authenticity and integrity of electronic messages affixed to electronic signatures. *Id.*; *see also* Stephen E. Blythe, *Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality*, 33 OHIO N. U. L. REV. 525 (2007).

101. *See* Blythe, *Digital*, *supra* note 97.

102. Stephen E. Blythe, *Cyber-Law of Japan: Promoting E-commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access*, 10 No. 1 J. INTERNET L. 20 (2006).

103. Stephen E. Blythe, *South Pacific Computer Law: Promoting E-commerce in Vanuatu and Fighting Cyber-Crime in Tonga*, 10 No. 1 J. S. PAC. L. 20 (2006), *archived at* http://www.webcitation.org/5UvBhOGBq.

104. Stephen E. Blythe, *Taiwan's Electronic Signature Act: Facilitating the E-commerce Boom with Enhanced Security*, THE SIXTH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON BUSINESS, Honolulu, Hawaii U.S.A., May 25-28, 2006.

105. Stephen E. Blythe, *Computer Law of Tunisia: Promoting Secure E-commerce Transactions with Electronic Signatures*, 20 No. 3 ARAB L. QUARTERLY 240 (2006).

106. Stephen E. Blythe, *Lithuania's Electronic Signature Law: Providing More Security in E-commerce Transactions*, 8 BARRY L. REV. 23 (2007).

107. Stephen E. Blythe, *Tehran Begins to Digitize: Iran's E-commerce Law as a Hopeful Bridge to the World*, 18 SRI LANKA J. OF INT'L L. 23 (2006).

108. 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 HOUS. J. INT'L L. 573 (2006).

109. Stephen E. Blythe, *The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute*, 16 CARRIBEAN L. REV. 149 (2007).

110. Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. *See* Blythe, *Hong Kong*, *supra* note 58.

111. *See* Fischer, *supra* note 61, at 234.

112. Stephen E. Blythe, *Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce*, 2:2 J. OF ISLAMIC STATE PRACTICES IN INT'L L. (2006).

113. Stephen E. Blythe, *The Dubai Electronic Transactions Statute: A Prototype for E-commerce Law in the United Arab Emirates and the G.C.C. Countries*, 23:1 J. OF ECON. & ADMIN. SCIENCES (2007).

114. Stephen E. Blythe, *Azerbaijan's E-commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region*, 1 COLUM. J. E. EUR. L. 44 (2007).

115. Stephen E. Blythe, *China's New Electronic Signature Law and Certification*

V. The Electronic Transaction Ordinance

The Electronic Transactions Ordinance[116] was drafted by the Nepal Ministry of Science and Technology and became law on September 15, 2004 by virtue of the decree of King Gyanendra.[117]

A. Purposes of the ETO

The purposes of the ETO are: (1) to attain integrity and reliability in the creation, production, processing, storage, communication and dissemination of electronic records[118], resulting in (2) more reliable and secure e-commerce transactions[119], and (3) to prevent unauthorized access or tampering with electronic records.[120]

The ETO would be strengthened with the addition of this statement:

If any other law of Nepal conflicts with the ETO, the ETO will prevail.[121]

B. Definitions

Significantly, there is no definition of an "electronic signature." This is perhaps the most telling indicator that Nepal remains in the First Generation of e-signature laws.[122] **An inclusive definition of an electronic signature**[123] **needs to be added. Nepal needs to jump from**

Authority Regulations: A Catalyst for Dramatic Future Growth of E-commerce, 7 CHI.-KENT J. INTELL. PROP. 1 (2007).

116. ETO, *supra* note 42.

117. ETO, *supra* note 42, Preamble, § 79.

118. *See* ETO, *supra* note 42, Preamble.

119. *See* L.D. Mahat, *Cyber Law to Support e-banking*, eKantipur.com (2004), *archived at* http://www.webcitation.org/5UwpBhOgV (discussing how digital signatures and the ETO will facilitate the growth of E-banking in Nepal).

120. *See* ETO, *supra* note 42. For an evaluation of the ETO, *see* Bashu Dev Phulara, *Nepalese Cyber Law Pros and Cons*, THE RISING NEPAL, Jan. 17, 2005.

121. *See, e.g.*, Electronic Transaction Law, 5/2004, ch. 13, ¶51 (2004) (Myan.) *archived at* http://www.webcitation.org/5Uwr3I5OT ("Notwithstanding anything contained in any existing law, the provisions contained in this Law shall prevail over the provisions not in conformity with or contradicting any provisions contained in this Law.").

122. *See* discussion *supra* Part IV.A.

123. For example, Hungarian law defines an electronic signature as "data in electronic form which are attached to or logically associated with other electronic data or which serve as a method of authentication." Act XXXV of 2001 on Electronic Signatures, §2(6) (2001) (Hung.), *archived at* http://www.webcitation.org/5UwtZ0zq3. This is an inclusive definition and is

the First Generation to the Third Generation of e-signature Laws by providing legal recognition to many types of e-signatures, while continuing to give most-favored-status to the digital signature.[124]

Nepal should consider adding a definition for the "owner" of an e-document. This would help to distinguish the owner in those situations when the owner is using an agent for his subscriber who is doing the "signing" on behalf of his principal, the owner. Under Bulgarian law, for example, if the sender of an electronic message is acting for himself and not on behalf of another party, the sender is referred to as the "titular." Sometimes, however, a natural person who sends an electronic message may be acting on behalf of another party, the principal. Although the agent must be a natural person, the principal could be either another natural person or a corporate entity. In principal-agent situations, Bulgarian law refers to the agent as the "author," but the principal is referred to as the "titular" of the electronic message.[125]

C. Extra-Territorial Jurisdiction

Nepal asserts jurisdiction over all parties committing crimes which target any computer system or computer network located within Nepal.[126] Not only does the ETO apply to wrongful acts committed inside Nepal, it also applies to wrongful acts affecting Nepal that are committed by persons outside of Nepal.[127] This jurisdiction is asserted over all violators, even if they reside outside of Nepal.[128] Because the internet is an international phenomenon, with stranger-parties doing business with each other across international boundaries, assertion of extra-territorial jurisdiction is easier to justify than in many other situations.[129]

evidence of technological open-mindedness.

124. Notwithstanding its affiliation with the First Generation of e-signature laws, the ETO does not appear to be as technologically-restrictive as some other jurisdictions. For example, it does 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. *See* UTAH CODE ANN. § 46-3-101, *supra* note 90. Private parties are allowed to make their own agreement pertaining to the requirements of creation of e-messages or e-documents. ETO, *supra* note 42, § 72.

125. Law for the Electronic Document and Electronic Signature, art. 4, (2001) (Bulg.), *archived at* http://www.webcitation.org/5WqL7Jts4.

126. ETO, *supra* note 43, § 55.

127. ETO, *supra* note 43, § 55.

128. ETO, *supra* note 43, § 55.

129. ETO, *supra* note 43, § 55 (Nepal asserts "long-arm" jurisdiction, even over foreign parties, so long as the "minimum contacts" are met, i.e., the target was a computer system or network located in Nepal).

This is a positive aspect of the ETO. It is a good idea for an electronic transactions law to explicitly claim "long-arm" jurisdiction over foreign parties engaging in e-commerce with parties in Nepal. Most of the world's electronic transaction laws fail to do this. The advantage to Nepal is that it places foreign parties on definite notice that they will be subject to the ETO and other pertinent laws of Nepal, and should facilitate the prosecution of criminal offenses against foreign parties in the Nepalese courts.[130]

D. Authentication of Electronic Records

In order for a subscriber to authenticate an electronic message or an electronic record, his digital signature must be affixed to said message or record.[131] An asymmetric crypto system must be used in conjunction with a hash function[132] to transform the original record.[133] It will be virtually impossible to compute or determine the original record from the hash function without the public key.[134]

E. "Secure" Digital Signatures and "Secure" Electronic Records

Digital signatures, examined and confirmed using the prescribed security procedures, will have "secure" status.[135] In order for an electronic message or another form of electronic record to have "secure" status, it must have been verified so there is assurance that the message or electronic record has not been altered since its creation.[136]

F. Legal Recognition of Electronic Records

130. Other jurisdictions explicitly claiming "long arm" jurisdiction against foreign parties include Singapore and Tonga. *See* Computer Misuse Act ch. 50A, §11 (1995) (Sing.); Computer Crimes Act of 2003, No. 14 § 3, (2003) (Tonga). *See also* Blythe, *Singapore*, *supra* note 101; Blythe, *South Pacific*, *supra* note 104, at 20-26.

131. ETO, *supra* note 43, § 3(1).

132. Hash function refers to the "acts of mapping of algorithm or translating of a sequence of bits into another, generally smaller, set yielding the same hash result from any record in the same form while executing the algorithm each and every time by using the same record as an input, infeasible to derive or reconstruct any record from the computation point of view, and making the two records, which produce the same hash result by using the algorithm, computationally infeasible to derive." ETO, *supra* note 43, § 3(2).

133. ETO, *supra* note 43, § 3(2).

134. ETO, *supra* note 43, § 3(3).

135. ETO, *supra* note 43, § 9.

136. ETO, *supra* note 43, § 8.

"Secure" electronic records and "secure" digital signatures, accorded that status using the verification method just described, are given legal status equivalent to records in paper form and to a pen-and-ink signature, respectively.[137]

Equivalent legal status is only given to those electronic documents that have been verified with the asymmetric crypto system that is associated with a digital signature. Likewise, an e-signature has equivalent legal status to an ink signature only if it has been attached to an electronic document using the same type of asymmetric crypto system.[138]

Nepal should add a paragraph pertinent to admissibility and weight of electronic evidence. The Barbadian statute is illustrative of good practice.[139]

More detailed rules regarding the presumptions of authenticity of e-documents and advanced e-signatures are also needed. For example, in Bahraini legal proceedings there is a rule that the information contained in an e-document is presumed to be authentic and is presumed not to have been altered unless evidence is presented to show that: (1) unreliable methods of creation, retention or transmission of the e-document were used; (2) an unreliable method of execution of the e-document was employed; (3) the integrity of the information contained in the e-document was not properly maintained; or (4) other relevant factors indicate that the e-document does not have integrity.[140] **Furthermore, in Bahraini**

137. ETO, *supra* note 43, §§ 4-5.

138. The ETO uses the term "secured" digital signature, but the European Union's E-Signatures Directive uses the term "advanced." *See* Council Directive 1999/93, *supra* note 43, at 14. Advanced E-signatures are admissible in legal proceedings and are defined to require: (1) a unique link to the signatory; (2) capability of identification of the signatory; (3) creation using means solely controlled by the signatory; and (4) linkage to the data in a manner whereby the recipient is able to detect any alterations to the original document sent by the signatory. *Id.*, art. 2(2)(a)-(d). *See* Blythe, *Digital*, *supra* note 98, at 21.

139. In Barbados, electronic records may not be denied admission into evidence in a court of law merely because of their electronic form. Factors to be taken into account by the court in its determination of whether to admit electronic evidence include: (1) the reliability of the means of creation, retention or communication of the electronic record; (2) the reliability of the means used to ensure that the information in the electronic record was not modified; (3) the means used to identify the electronic record's creator; and (4) "any other relevant factor." Electronic Transactions Act, L.R.O. 2001, Ch. 308, §§ 11(1)-(2) (Barb.) [hereinafter Barbados Act], *archived at* http://www.webcitation.org/5V2q43pBR. *See* Blythe, *Barbados*, *supra* note 110.

140. *See* Legislative Decree No. 28 with Respect to Electronic Transactions, art. 5(4), (2002) (Bahr.)
archived at http://www.webcitation.org/5V2qriqdN [hereinafter Bahrain Legislative Decree No. 28]. Of course, notwithstanding the presumption, a legal

legal proceedings an e-signature supported with a qualified certificate is presumed to be: (1) authentic, (2) the signature of the person it purports to be associated with, (3) attached by that person to an e-document in order to show that they signed the e-document, and (4) an unaltered e-document which has not been modified since the time the e-signature was attached to it. To overcome this legal presumption parties must have stipulated otherwise or shown that evidence to the contrary exists.[141] **However, this legal presumption does not apply to an e-signature that is not supported with a qualified certificate.**[142]

1. Electronic Record Complies With Paper Copy Requirement

If a law requires that an e-document must be in "hard" form, secure electronic records may be used instead of paper, provided that all requirements of the ETO have been complied with.[143] In other words, secure electronic records are the legal equivalent of paper records.

The ETO, however, allows a number of exclusions from coverage by the statute. Similarly to most other e-commerce laws worldwide, Nepal recognizes the necessity of requiring traditional paper documents in some situations, such as: (1) negotiable instruments[144], (2) documents pertaining to ownership or transfer of real property (e.g., deeds, contracts of sale of land and dwellings, mortgages, leases, easements, and partitions)[145], (3) documents pertaining to ownership of other types of immovable property[146], (4) documents required to be filed in court (e.g., lawsuits and powers of attorney)[147], (5) documents required to be submitted at arbitration proceedings[148], and (6) any other documents required by law not to be retained in electronic form.[149] Furthermore, the government reserves the right to add or remove items from this list by publication in the *Nepal Gazette*.[150]

challenge to the authenticity and integrity of an e-document could be made in court. *Id.* at art. 22.

141. *Id.* at art. 6(3). Notwithstanding the presumption, a legal challenge to the authenticity and integrity of an E-signature could be made in court. *Id.* at art. 22.

142. *Id.* at art. 6(4).

143. ETO, *supra* note 43, § 4.

144. ETO, *supra* note 43, § 77(1)(a). The negotiable instruments required to be in paper form are defined in the Negotiable Instruments Act 2034, (1977) (Nepal).

145. ETO, *supra* note 43, § 77(1)(b).

146. ETO, *supra* note 43, § 77(1)(c).

147. ETO, *supra* note 43, § 77(1)(d).

148. ETO, *supra* note 43, § 77(1)(e).

149. ETO, *supra* note 43, § 77(1)(f).

150. ETO, *supra* note 43, § 77(2).

This is a negative aspect of the ETO. Internationally, exclusions from coverage are slowly being eliminated.[151] **Although Nepal's number of exclusions is small in comparison with some jurisdictions**[152]**, it could be reduced. A good beginning would be to allow electronic filing of court documents. It is commendable, however, that wills, codicils and testamentary trusts are not included in the list. In many jurisdictions, wills and related documents must be in writing and the electronic form is not recognized.**[153]

151. *See* Electronic Document Law, art. 1.1, (2003) (Azer.), *archived at* http://www.webcitation.org/5V2rQMxSS; Law on Electronic Signature, No. VIII—1822 (2000) (Lith.), as amended: No. IX—934 (2002) (Lith.), *archived at* http://www.webcitation.org/5V2rJdaI4; Law Regulating Digital Signatures and Certificates (2000) (Peru), *translated by* National Law Center for Inter-American Free Trade, *archived at* http://www.webcitation.org/5V2rCgaA4. Azerbaijan is perhaps the most progressive nation in the world in terms of exclusions. Its Electronic Document Law lists no exclusions and states that e-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." Electronic Document Law, art. 1,1. Peruvian and Lithuanian statutes also do not contain exclusions from coverage. *See also* Blythe, *Tehran*, *supra* note 108; Blythe, *Lithuanian*, *supra* note 107, at 40.

152. *See* Blythe, *Critique*, *supra* note 96, at 37. Hong Kong, for example, lists the following exceptions: wills, codicils and other testamentary documents; anything to do with the creation, change or revocation of an express trust; a power of attorney; documents required to be stamped pursuant to the Stamp Duty Ordinance (Cap. 117); Government grants and leases; deeds, conveyances, judgments, written instruments, *lis pendens* and documents effecting a floating charge pursuant to the Land Registration Ordinance; assignments, mortgages and legal charges under the Conveyancing and Property Ordinance; oaths and affidavits; statutory declarations; judgments or orders of a court; warrants issued by a court or a magistrate; negotiable instruments; and any documents applicable to matters coming before the following courts, government agencies or government officials: the Court of Final Appeal; the Court of Appeal; the Court of First Instance; the District Court; the Mental Health Review Tribunal established pursuant to the Mental Health Ordinance; the Lands Tribunal; a coroner appointed under s.3 of the Coroners Ordinance; the Labour Tribunal; the Obscene Articles Tribunal established under the Control of Obscene and Indecent Articles Ordinance; the Small Claims Tribunal; and a magistrate. Hong Kong Special Autonomous Region, Electronic Transactions Ordinance, Ord. No. 1 of 2000, Schedules 1 and 2. For a discussion of the Hong Kong exclusions, *see* Blythe, *Hong Kong*, *supra* note 58.

153. *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 U. MEM. L. REV. 603 (2005). There is evidence that 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. This case recognized that a computer-generated signature may be used by a testator to "sign" the document. The testator had affixed the electronic signature in the presence of two witnesses. The appellate court held that "[a] computer-generated signature made by a testator

2. E-Signature Complies with Requirement of a Pen-and-Paper Signature

If a law requires that a signature must be affixed with ink signed on paper, a secure digital signature may be used instead of the ink and paper, provided that all requirements of the ETO have been complied with.[154]

Only the digital signature may be used to meet a statutory requirement for an ink signature. This is further evidence that the ETO is a member of the first generation.[155]

3. Electronic Form Complies with Retention Requirement

If any law mandates that paper documents or records must be retained for a minimum period of time, said documents or records may be in electronic form if the following criteria are met:

a. The documents or records are easily accessible; and
b. The format is the same as the original, or in a form providing an accurate representation of the information in the original document or record; and
c. The electronic document or record includes information pertaining to the "origin, destination and transmission or date and time of receipt." However, this third requirement does not apply to any automatically-generated computer information which is only for the purpose of the sending or receiving of the document or record.[156]

4. Electronic Form Complies with Original Document Requirement

If a law requires that a document must be submitted in its original form[157], or must be retained in its original form, then an electronic record will fulfill this requirement if the following criteria are met:

a. No evidence exists to indicate that the electronic record has

comes within the description of 'any other symbol or methodology executed or adopted by a party with intention to authenticate a writing or record,' and if affixed before two or more attesting witnesses, satisfies the requirements for a testator to execute a will.'" *Id.* at 604, citing Taylor v. Holt, 134 S.W.3d 830, 834 (Tenn. Ct. App. 2003).

154. ETO, *supra* note 43, § 5.
155. For discussion on the "First Generation", *see supra* Part IV.A.
156. ETO, *supra* note 42, § 6.
157. E.g., as in a legal proceeding in a court of law.

been altered since the time of its creation; and

b. It is possible for the electronic record to be "clearly shown" to the person or tribunal that the law requires it to be shown to.[158]

A provision allowing delivery of an e-document to comply with the statutory requirements for delivery of a paper document is needed.[159] **Also needed is a provision allowing compliance with statutory notarization requirements if the authorized e-signature is attached to an e-document.**[160] **Finally, the ETO should allow the presentation of only one e-document to a person in order to comply with any statutory requirement to present one or more copies of a paper document to that person.**[161]

G. Electronic Contract Rules

1. Attribution

It shall be assumed that an electronic record is the sender's, if the following criteria are met:

a. The sender personally sent the record; or
b. The sender's agent sent the record; or
c. The sender's computer system, which had been programmed by the sender (or his agent), automatically sent the record.[162]

In a principal-agent situation, it is important to distinguish the principal or owner of an electronic record from his agent.[163]

If the parties placed any conditions upon the assumption of attribution by the receiver, and those conditions exist, then the receiver may assume the sender did in fact, send the electronic document.[164]

Rules are needed as to when the receiver may assume that a

158. ETO, *supra* note 43, § 7.
159. *See* Blythe, *Critique*, *supra* note 96, at 24. In Barbados, if a statute mandates that information is to be delivered from one party to another, that mandate is deemed to have been met if: (1) an electronic record containing the information is sent from the sender, requesting acknowledgement of receipt from the receiver; and (2) the receiver acknowledges the receipt to the sender. *See generally* Blythe, *Barbados*, s*upra* note 110. This applies regardless of whether there is an affirmative obligation for the information to be delivered, or there will be adverse consequences if the information is not delivered.
160. UNIFORM ELECTRONIC TRANSACTIONS ACT, § 11 (1999), *archived at* http://www.webcitation.org/5VL2S2nQZ; s*ee also* Blythe, *Barbados*, s*upra* note 110.
161. *See* Bahrain Legislative Decree No. 28, *supra* note 141, at art. 8.
162. ETO, *supra* note 42, § 10(1).
163. *See* discussion *supra* Part V.B.
164. ETO, *supra* note 42, § 10(2).

particular sender transmitted the message[165] **and as to whether the receiver may assume that the message received is what the sender intended to send.**[166] **Rules regarding the receipt of duplicate messages are also needed.**[167]

2. Acknowledgement of Receipt

165. *See* Blythe, *Singapore*, *supra* note 100, at 536. "A receiver may assume that a received message was sent by the sender if: (1) a procedure-previously agreed to by the sender-was applied by the receiver to ascertain whether the sender actually sent the message, and the procedure confirmed that was the case; or (2) the data in the message which was received indicated they were the product of the sender, using an identification method that could have been known only to the sender, her agent, or by someone having a close relationship with the sender or the agent…The rules in the preceding paragraph are inapplicable if: (1) the receiver was in receipt of a timely notice from the sender that said electronic record did not belong to her or her agent; (2) the receiver either knew, or should have known if reasonable care or a specifically-agreed procedure had been employed, that the electronic record did not belong to the sender or her agent; or (3) considering all aspects of the particular case, it is "unconscionable" for the receiver to assume that the electronic record belonged to the sender or her agent or act on such an assumption." *Id.; See also* Electronic Document and Electronic Signature, SG 34 Art. 15 (2001) (Bulg.) *archived at* http://www.webcitation.org/5V47nig1w. Bulgaria has rules regarding a subscriber's disavowal or contesting of the authenticity of his electronic signature. A subscriber is not allowed to disavow an electronic document signed with his electronic signature whenever: (1) the electronic document was transmitted through an automated computer information system; or (2) the electronic document was sent to an addressee to whom the means of access of identification had been given by the subscriber to another party. *Id*. In the second case, contesting is allowed by the subscriber from the point in time that the addressee receives notice that the electronic document did not emanate from the subscriber, and the addressee has sufficient time to adjust his behavior accordingly. *Id*. Additionally, contesting is allowed by the subscriber in both the first and second situations whenever the addressee has failed to exercise reasonable care. *Id*.

166. *See* Singapore Electronic Transactions Act, *supra* note 100, § 13(6). In Singapore, whenever the received message: (1) is the sender's; or (2) is legally considered to be the sender's; or (3) is assumed to be that of the sender, and receiver is entitled to act on that assumption: Then, the receiver may assume that the message is what the sender intended to send, and may act on that assumption. The preceding rule is inapplicable if the receiver either knew, or should have known if an agreed-on-procedure or reasonable care had been employed, that there was an error in the transmission of the message. Blythe, *Singapore*, *supra* note 100, at 536.

167. *See* Singapore Electronic Transactions Act, *supra* note 100, § 13(7). Ordinarily the receiver may assume that each electronic message received is independent of the others, and that no duplicate messages were sent by the sender. However, if the receiver mistakenly makes a duplicate of an electronic message, it may not be considered to be a new independent message if the mistake would not have occurred if the receiver had taken reasonable care or if the receiver had employed a previously-agreed-to procedure.
Blythe, *Singapore*, *supra* note 100, at 536-37.

Acknowledgement is a confirmation of receipt from the message recipient to the message sender. The following rules are applicable only if: (1) the sender requests confirmation of receipt before or during the transmission of the message, or (2) the sender and receiver have agreed that acknowledgement must be given.[168]

a. If the parties have not agreed as to the specific form or method of acknowledgement, then the receiver is free to choose any form or method, automated or non-automated, or the receiver may use any actions which will sufficiently indicate to the sender that the message has been received.[169]
b. If the sender has informed the receiver that the electronic record will be "binding" only upon acknowledgement, then if no acknowledgement is received by the sender, it shall be assumed that the electronic record was never sent.[170]
c. If the sender has not indicated that the document will be "binding" only on receipt of confirmation, and the parties have not agreed as to a particular time for a confirmation, then the acknowledgement must be received by the sender "within a specified time as prescribed"[171] for it to be deemed to have been sent by the sender.[172]
d. The Controller may issue additional rules pertaining to the acknowledgment of electronic records.[173]

The ETO fails to cover whether the mere receipt of an acknowledgement from the receiver is sufficient evidence for the sender to assume that the message received is identical to what was sent.[174]

3. Time/Place of Dispatch/Receipt

The parties may stipulate to the time and place that a message will be deemed sent and received. If so, those stipulations will be controlling and override the rules below.[175]

168. ETO, *supra* note 43, § 11(1).
169. ETO, *supra* note 43, § 11(2).
170. ETO, *supra* note 43, § 11(3).
171. ETO, *supra* note 43, § 11(4). The Controller may issue a regulation as to the "prescribed" time. *Id*.
172. ETO, *supra* note 42, § 11(4).
173. ETO, *supra* note 43, § 11(5).
174. *See* Barbados Act *supra* note 140, § 14(4). In Barbados, the acknowledgment is insufficient legal evidence for the sender to assume that the content of the electronic message received by the receiver is identical to what was sent by the sender. *Id*. *See also* Blythe, *Barbados*, *supra* note 80.
175. ETO, *supra* note 43, §§ 12(1)-(3).

a. An electronic record will be deemed dispatched when it enters a computer system outside the control of the sender.[176]
b. The time of receipt of an electronic record "shall be determined as prescribed."[177]
c. The default place of dispatch shall be the sender's place of business, and the default place of receipt shall be the recipient's place of business.[178] If a party has more than one place of business, it shall default to the place of business "concerned" with the particular electronic communiqué.[179] If a party does not have a place of business, it shall be assumed to be their "place of residence."[180]

The ETO fails to ascertain the time of dispatch when both sender and recipient use the same computer information system.[181]

H. Appointment of Regulator

The King of Nepal may appoint a governmental officer to hold the post of Controller.[182] The Controller, along with Deputy Controllers appointed by the Controller,[183] will have the general responsibility of regulating the Certifying Authorities.[184]

With respect to CA's, the Controller will have the following specific responsibilities:

a. licensing of CA's;[185]
b. supervising the CA's and controlling how they conduct their business;[186]
c. development and dissemination of standards to be applied by

176. ETO, *supra* note 43, § 12(1).
177. ETO, *supra* note 43, § 12(2). The Controller will issue a regulation pertaining to the assumed time of receipt of an electronic record. *Id*.
178. ETO, *supra* note 43, § 12(3).
179. ETO, *supra* note 42, § 12(3)(a).
180. ETO, *supra* note 43, § 12(3)(b).
181. *See* Bahrain Legislative Decree no. 28, *supra* note 141, at art. 15(1)(ii). In Bahrain, if the parties are using the same computer information system, transmission of an e-message is deemed to have occurred "when it comes to the attention of and becomes capable of being retrieved by the addressee." *Id*.
182. ETO, *supra* note 42, § 13(1). Mr. Deepak Rauniar became the first appointed Controller. *Government to Introduce Law on Electronic Transaction*, LEGAL NEWS FROM NEPAL, April 1, 2006, at 1, *archived at* http://www.webcitation.org/5V4E4u4sl. It is unknown at this time how the removal of Nepal's monarchy will effect this provision. *See* discussion *supra* Part II.C.
183. ETO, *supra* note 42, § 13(2).
184. ETO, *supra* note 43, § 14.
185. ETO, *supra* note 43, § 14(a).
186. ETO, *supra* note 43, §§ 14(b), (d).

CA's in the verification of digital signatures;[187]

d. informing the CA's as to the form of the certificates they issue, and the required information included in the certificates;[188]
e. regulating the relationship between the CA and its subscribers;[189]
f. maintaining an up-to-date database of information pertaining to CA's and the certificates they have issued;[190] and
g. performing other duties as directed.[191]

I. Regulation of Certifying Authorities

1. The CA Must Have A License

No business may act as a CA unless it holds a license issued by the Controller.[192]

This is sometimes referred to as a "compulsory"[193] CA system because holding a license is a requirement. A compulsory system is preferable to a voluntary one because it facilitates the attainment of a greater degree of regulation by the Controller.[194]

187. ETO, *supra* note 43, § 14(c).
188. ETO, *supra* note 43, § 14(e).
189. ETO, *supra* note 43, § 14(f).
190. ETO, *supra* note 43, § 14(g). The database is ordinarily available for public viewing at the Controller's website.
191. ETO, *supra* note 43, § 14(h).
192. ETO, *supra* note 43, § 15.
193. China and Dubai are examples of other jurisdictions with a compulsory CA system. Order (No. 18) of the President of China, LAW ON ELECTRONIC SIGNATURE, [hereinafter China Law on Electronic Signatures] Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress of China (promulgated 28 August 2004, effective 1 April 2005) *archived at* http://www.webcitation.org/5V4FIBFGt. The Law was translated into English by the Beijing University School of Law, Beijing, China. *See also* LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE No. 2/2002 (2002) (Dubai); *archived at* http://www.webcitation.org/5V4FXkHq9; Blythe, *Dubai*, *supra* note 113; Blythe, *China*, *supra* note 114.
194. Some other jurisdictions, e.g. Hong Kong and Pakistan, have a voluntary CA system, allowing the possibility of having unlicensed certification business firms. A common disadvantage of such unlicensed firms, however, is that their verification of e-documents and e-signatures may carry less legal significance that that of a full-fledged, licensed CA. *See* Hong Kong Special Administrative Region: Electronic Transactions Ordinance, No. 1 (2001), *archived at* http://www.webcitation.org/5V4GjnZdG;. *See also* Electronic Transactions Ordinance (2002) (Pak.), *archived at* http://www.webcitation.org/5V4GvHZ3d; Blythe, *Hong Kong*, *supra* note 58; Blythe, *Pakistan*, *supra* note 112.

2. Application Requirements

In order to be considered for the issuance of a CA's license,[195] an applicant must submit the following to the Controller:

a. an executed application form to be provided by the Controller;[196] and
b. the application fee to be prescribed by the Controller;[197]

The amount of the financial resources required to be held by the CA is not specified. In some jurisdictions, the amount is specifically listed, e.g., China[198] and India.[199] It is a good idea to mandate that the CA have a relatively high, specific amount of capitalization in order to protect the subscriber in case the CA becomes liable for damages. Alternatively, the statute could require the CA to carry a specific amount of insurance coverage.

c. the applicant's Certification Practice Statement (hereinafter "CPS");[200]

The contents of the CA's Certification Practice Statement should be addressed.[201]

d. documents to verify the applicant's identity;[202]

195. ETO, *supra* note 42, § 16.
196. ETO, *supra* note 43, § 16(1).
197. ETO, *supra* note 43, § 16(1).
198. China Law on Electronic Signatures, *supra* note 193, at ch. III.
199. The Information Technology Act, No. 21 of 2000; India Code (2000), § 21, *archived at* http://www.webcitation.org/5WqKWMBBS [hereinafter Information Technology Act]; *see also* Blythe, *Critique*, *supra* note 95.
200. ETO, *supra* note 43, § 16(2)(a). The idea of a Certification Practice Statement ("CPS") originated in the United States. The prospective CA, or licensed CA, must draft the CPS. The CPS will contain the detailed policies, procedures and rules which the CA expects to implement in the execution of its duties and responsibilities. *See* ABA, *supra* note 62, at 29.
201. In Taiwan, for example, a licensed CA is not allowed to begin issuing certificates to the public until it has filed a CPS with the Ministry of Economic Affairs, and it has been approved. The Ministry will publish a list of the CA firms that have filed an approved CPS. A CPS contains the practices and procedures employed by a CA in the issuance of Certificates and in other certification-related services. After approval of the Ministry has been obtained, the CPS must be published on the CA's website and made available to the general public. If modifications are made to the CPS, they must also be approved by the Ministry and published on the website. The CPS must contain the following: (1) information pertaining to the trustworthiness of the CA's operations or the Certificates it has issued; (2) grounds which would justify the CA to unilaterally revoke a Certificate; (3) how the Certificate-related information will be retained and may be accessed; (4) methods used to protect the subscribers' personal information; and (5) other important information to be determined by the Ministry of Economic Affairs. Electronic Signatures Act art. 11-12 (2002) (Taiwan), *archived at* http://www.webcitation.org/5VuDMuie7; *see also* Blythe, *Taiwan*, *supra* note 105.
202. ETO, *supra* note 43, § 16(2)(b).

e. statements of the applicant's human, financial and physical resources;[203] and
f. other documents as the Controller may require.[204]

3. The Licensing Procedure

Within two months after receipt of the application, the Controller must decide whether the application will be accepted or rejected.[205] In making the decision, the Controller should consider the sufficiency of the applicant's human, financial, physical and other resources.[206] The Controller may inspect the applicant's proposed business site and check on the applicant's financial and physical resources.[207] If the Controller decides to reject the application, the applicant must be so informed.[208] If the Controller decides to issue the license, the license document must have a prescribed format and the date of issuance and the date of expiration.[209] The new licensee should be informed of any terms or conditions which may affect the validity of the license.[210] Other procedures may also be required to complete the licensing process.[211] If issued, the license will be valid for a period of one year.[212]

4. License Renewal

A CA must renew its license every year.[213] This application for renewal shall be filed with the Controller at least two months before the expiration date of the license.[214] The application must be made on the form prescribed by the Controller and a renewal fee paid.[215] The Controller must make decide whether to renew at least one month before the current license is due to expire.[216] If the Controller decides to reject the application for renewal, the applicant should be afforded a

203. ETO, *supra* note 43, § 16(2)(c). The Controller may inspect the applicant's facilities before issuance of the license. *Id.* § 18(2).
204. ETO, *supra* note 43, §§ 16(2)(d), 16(3).
205. ETO, *supra* note 43, § 18(1).
206. ETO, *supra* note 43, § 18(1).
207. ETO, *supra* note 43, § 18(2).
208. ETO, *supra* note 43, § 18(1).
209. ETO, *supra* note 43, § 18(3).
210. ETO, *supra* note 43, § 18(3).
211. ETO, *supra* note 43, § 18(4).
212. ETO, *supra* note 43, § 19(1).
213. ETO, *supra* note 43, § 19(1).
214. ETO, *supra* note 43, § 19(2).
215. ETO, *supra* note 43, § 19(2).
216. ETO, *supra* note 43, § 19(3).

"reasonable opportunity" to make a pertinent statement in rebuttal.[217]

5. License Suspension

The Controller has the authority to suspend a CA's license if it:

a. made a false statement or submitted false documents in the application, e.g., misrepresentation of financial or physical resources;[218] or
b. did not comply with its own CPS;[219] or
c. violated any part of the ETO or its implementation regulations;[220] or
d. for other reasons to be prescribed by the Controller.[221]

The CA should be given a reasonable opportunity to make a statement in rebuttal before the suspension becomes effective.[222]

If suspension occurs, the Controller is required to give written notice to the CA and to keep an electronic copy of said notice in its database.[223] Furthermore, the Controller shall give notice of the suspension to the general public by two means: (1) on its website;[224] and (2) publication on two occasions in two newspapers (one Nepalese language, one English language).[225] *But Note*: Third-party claims of adverse effect due to lack of notice of the suspension will not be countenanced.[226]

6. License Revocation

The Controller may revoke a CA's license if the CA:

a. refuses to recognize or comply with any liabilities it has incurred by virtue of the ETO or its implementation regulations;[227] or
b. made false or misleading statements or submitted false or misleading documents in its original application or for renewal of the license;[228] or
c. has conducted its business in a manner detrimental to the

217. ETO, *supra* note 43, § 19(4).
218. ETO, *supra* note 43, § 20(1).
219. ETO, *supra* note 43, § 20(1).
220. ETO, *supra* note 43, § 20(1).
221. ETO, *supra* note 43, § 20(2).
222. ETO, *supra* note 43, § 20(1).
223. ETO, *supra* note 43, § 22(1).
224. ETO, *supra* note 43, § 22(1).
225. ETO, *supra* note 43, § 22(2).
226. ETO, *supra* note 43, § 22(2).
227. ETO, *supra* note 43, § 21(1)(a).
228. ETO, *supra* note 43, § 21(1)(b).

public interest or the national economy;[229] or

d. has committed an offense[230] listed in the ETO or its implementation regulations.[231]

Before the revocation is affected, the CA must be given a "reasonable opportunity" to make a statement to the Controller in rebuttal.[232] The Controller may also prescribe other procedures pertaining to revocation.[233] If revocation occurs, the Controller must give written notice to the CA and keep an electronic copy of said notice in its database.[234] Furthermore, the Controller shall give notice of the revocation to the general public: (1) on the Controller's website;[235] and (2) by publication on two occasions in two newspapers (one Nepalese language, one English language).[236] *But Note:* Third-party claims of adverse effect due to lack of notice of the revocation will not be countenanced.[237]

A provision stating that a CA is free to go out of business after receiving the Controller's approval is needed. Further, the Controller should be required to publish notice of the retiring CA.[238]

7. Recognition of Foreign CA's

A party holding a CA's license issued in a foreign country may also be allowed to issue certificates in Nepal pursuant to the ETO, provided it has obtained approval and recognition from the Controller and the government of Nepal.[239] If approved, notification will be made by the Controller in the *Nepal Gazette*.[240] The Controller will issue regulations pertaining to the recognition of foreign CA's.[241]

Because e-commerce is inherently multi-jurisdictional, it is

229. ETO, *supra* note 43, § 21(1)(c).
230. Computer crimes are listed in Chapter 9 of the ETO. ETO, *supra* note 43, §§ 44-59.
231. ETO, *supra* note 43, § 21(1)(d).
232. ETO, *supra* note 43, § 21(2).
233. ETO, *supra* note 43, § 21(3).
234. ETO, *supra* note 43, § 22(1).
235. ETO, *supra* note 43, § 22(1).
236. ETO, *supra* note 43, § 22(2).
237. ETO, *supra* note 43, § 22(2).
238. Denshisyomei oyobi ninsyogyomu ni kansuru houritsu [Law Concerning Electronic Signatures and Certification Services], Law No. 102 of 2000, art. 10, *translation archived at* http://www.webcitation.org/5VJJPdhek. *See also* Blythe, *Japan*, *supra* note 103.
239. ETO, *supra* note 43, § 23(1).
240. ETO, *supra* note 43, § 23(1).
241. ETO, *supra* note 43, § 23(2).

critical for the ETO to sufficiently address recognition of foreign CA's and the certificates they have issued. Other jurisdictions have specified a number of methods for recognizing foreign CA's and foreign certificates.[242]

J. The Controller's Continual Oversight Activities

1. Controller's Issuance of Regulations

In the pursuit of overseeing CA activities, the Controller will continually issue regulations pertaining to new or recurring issues.[243] The Controller reserves the right to specify the "functions and duties" of the CA through issuance of these regulations.[244]

2. Controller's Right to Delegate to Others

The Controller reserves the right to delegate to subordinate officers any power or authority conferred upon him by the ETO or its implementation regulations.[245]

3. Controller's Investigative Powers

Pursuant to the ETO, the Controller may investigate any CA, subscriber, relying third party or other party under suspicion of violating the ETO or its implementation regulations.[246] The CA has the duty to cooperate with the Controller in the investigation.[247] The Controller

242. In Iceland, which recently became the "most wired" nation in the world in terms of percentage of the population that regularly connects to the Internet (almost 80%!), certificates issued by foreign CA's will be recognized as qualified certificates in Iceland provided: (1) the foreign CA is in compliance with Iceland's Electronic Signature Act ("ESA") requirements and approved by a "voluntary accreditation scheme" of the European Economic Area; (2) the foreign CA is licensed within the European Economic Area, is in compliance with the ESA requirements, and guarantees the certificate; (3) the foreign CA is licensed within the European Economic Area and is in compliance with its home country's criteria for qualified certificates; or (4) the certificate or the foreign CA has been approved in bilateral or multilateral treaties between Iceland, the European Union, nations outside the European Union, or international organizations. Merchants and Trade – Act On Electronic Signatures, Act No. 28/2001, Art. 22, (2001) (Iceland), *archived at* http://www.webcitation.org/5VJJcX0F2.

243. ETO, *supra* note 43, § 24.

244. ETO, *supra* note 43, § 17.

245. ETO, *supra* note 43, § 25.

246. ETO, *supra* note 43, § 26(1).

247. ETO, *supra* note 43, § 26(2).

may issue regulations pertaining to the investigatory procedures.[248]

4. Controller's Annual Audit of the CA

Every year, the Controller may conduct an audit of the CA's activities.[249] Outside auditors or experts in computer information systems or computer security may be appointed to conduct or assist in the audit.[250] The Controller will prescribe the minimal qualifications of these individuals, their remuneration, and the procedures to be employed in the conduct of the audit.[251] The results of the audit will be retained in the Controller's database, and made available for public viewing on the Controller's website.[252] One goal of the audit is ensure that all CA's services are based upon common standards, and the general public will be given notice of these standards.[253]

The annual audit is a positive aspect of the ETO and one that other jurisdictions should emulate. Although most jurisdictions provide for punitive measures against CA's that violate e-commerce and other laws, not enough nations periodically undertake an inspection of CA's to ensure that their business operations are being conducted properly.

5. Controller's Right of Access to CA's Computers and Electronic Records

In order for the Controller to effectively perform its oversight duties, he must have access to the CA's computer and records when there is reasonable cause to believe the CA has violated the ETO or its regulations.[254] Accordingly, the Controller may issue directives containing specific procedures mandating the cooperation of any party under investigation,[255] and the parties must cooperate fully.[256]

248. ETO, *supra* note 43, § 26(3).
249. ETO, *supra* note 43, § 27(1). One purpose of the annual audit is to determine whether each CA is in compliance with its own CPS. The CPS is a statement drafted by a CA containing its own specific policies, procedures and rules which are followed by the CA on a daily basis. One of the most significant parts of the CPS pertains to its practices concerning the issuance of certificates to subscribers. *Id*. § 2(s).
250. ETO, *supra* note 43, § 27(2).
251. ETO, *supra* note 43, § 27(4).
252. ETO, *supra* note 43, § 27(3).
253. ETO, *supra* note 43, § 27(5).
254. ETO, *supra* note 43, § 28(1). Arguably, this also extends to subscribers, relying third parties, and anyone else under suspicion of violation of the ETO or its regulations.
255. ETO, *supra* note 43, § 28(2)

6. Controller to Maintain Repository

The Controller will maintain a repository containing: (1) digital signature certificates issued pursuant to the ETO;[257] and (2) related public keys.[258] The Controller will employ security procedures to ensure the "privacy and integrity" of the digital signatures.[259] The public keys will be available in the Controller's database for public viewing.[260]

K. The Issuance of Certificates by CA's

Licensed CA's are the only entities empowered to issue a Digital Signature Certificate.[261]

1. Application for Certificate

An applicant seeking a digital signature certificate should apply to a CA.[262] The CA will inform the applicant of the fee, the application form to be used.[263] Within one month of receipt of the application, the CA must decide whether to accept or reject the application.[264] Upon acceptance, the CA must issue the certificate within seven days of the decision.[265] Alternatively, if the CA rejects the application, it must inform the applicant of the reasons for the rejection within seven days of the decision.[266]

2. Suspension of the Certificate

The CA may suspend a certificate on any of the following grounds:[267] (1) a request for suspension by the subscriber or his agent;[268] (2) when a

256. ETO, *supra* note 43, § 28(3).
257. ETO, *supra* note 43, § 29(1).
258. ETO, *supra* note 43, § 29(3).
259. ETO, *supra* note 43, § 29(2)(b).
260. ETO, *supra* note 43, § 29(4).
261. ETO, *supra* note 43, § 30. This is the essence of a compulsory system of CA licensing. *See* discussion Part V.I.1.
262. ETO, *supra* note 43, § 31(1).
263. ETO, *supra* note 43, § 31(1).
264. ETO, *supra* note 43, § 31(2).
265. ETO, *supra* note 43, § 31(3).
266. ETO, *supra* note 43, § 31(3).
267. ETO, *supra* note 43, § 32(1).
268. ETO, *supra* note 43, § 32(1)(a).

suspension would best serve the public interest;[269] or (3) when there is a possibility of "significant loss" to relying third parties due to failure to abide by the ETO or its regulations at the time the certificate was issued, and the Controller directs the CA to suspend.[270] The Controller will prescribe specific regulations pertaining to the suspension procedure.[271]

Notice of the suspension will be published on the Controller or CA's website, and a record of the suspension will be maintained in the repository of the Controller or the CA.[272] The Controller or CA should inform the subscriber of his certificate's suspension as soon as possible.[273]

3. Revocation of the Certificate

The Controller or CA may revoke any certificate on the following grounds:[274] (1) when the subscriber or her agent so requests;[275] (2) when this action would best serve the public interest;[276] (3) when the subscriber is deceased;[277] (4) when the subscriber becomes insolvent and has entered bankruptcy proceedings;[278] (4) when any requirement for issuance of the certificate has not been complied with;[279] (5) when a material fact the placed in the certificate is proven false;[280] or (6) when the CA's computer system or the private key is no longer secure, and this has had a material detrimental effect upon the reliability of the certificate.[281] The Controller may issue specific regulations pertaining to the revocation procedure.[282]

Notice of the revocation will be published on the Controller or CA's website, and a record of the revocation kept in the Controller or CA's repository.[283] The Controller or CA is responsible for informing the subscriber of the revocation as soon as possible.[284]

269. ETO, *supra* note 43, § 32(1)(b).
270. ETO, *supra* note 43, § 32(1)(c).
271. ETO, *supra* note 43, § 32(2).
272. ETO, *supra* note 43, § 34(1).
273. ETO, *supra* note 43, § 34(2).
274. ETO, *supra* note 43, § 33(1).
275. ETO, *supra* note 43, § 33(1)(a).
276. ETO, *supra* note 43, § 33(1)(b).
277. ETO, *supra* note 43, § 33(1)(c).
278. ETO, *supra* note 43, § 33(1)(d). This applies only if the subscriber is a company or corporate entity, not an individual. *Id.*
279. ETO, *supra* note 43, § 33(1)(e).
280. ETO, *supra* note 43, § 33(1)(f).
281. ETO, *supra* note 43, § 33(1)(g).
282. ETO, *supra* note 43, § 33(2).
283. ETO, *supra* note 43, § 34(1).
284. ETO, *supra* note 43, § 34(2).

L. The Subscriber's Rights and Responsibilities

1. Duty to Generate the Keys

If the subscriber generates the public and private key, then the subscriber must use the "secured asymmetric crypto system." [285] The public key, corresponding to the private key retained by the subscriber, will be listed in the certificate.[286] If the CA and the subscriber have agreed to use a specific type of security system for the private key, then the subscriber must employ said security system.[287]

2. Acceptance of the Certificate

A certificate is considered legally accepted from the CA when: (1) the subscriber or his agent presents it to one or more persons;[288] or (2) the subscriber has led other parties to rely on the information contained in the certificate.[289] To all persons who "reasonably rely" on the certificate's information, the subscriber warrants that: [290] (1) the subscriber holds the private key corresponding to the public key included in the certificate, and is entitled to hold it;[291] (2) all statements made to the CA are true, and all documentary evidence presented to the CA in the application process are valid;[292] and (3) to the best of the subscriber's knowledge, all information contained in the certificate is true.[293]

Prior to issuing the certificate, the CA should notify the subscriber of: (1) the certificate's terms and any limitations on usage; (2) information pertaining to the CA's accreditation; and (3) the customer complaint procedure.[294]

285. ETO, *supra* note 43, § 35(1). Secured asymmetric crypto system is defined as "a system that creates a secured key-pair consisting of a private key creating a digital signature and a public key to verify the digital signature." *Id.* § 2(a).
286. ETO, *supra* note 43, § 35(1).
287. ETO, *supra* note 43, § 35(2).
288. ETO, *supra* note 43, § 36(1)(a).
289. ETO, *supra* note 43, § 36(1)(b).
290. ETO, *supra* note 43, § 36(2).
291. ETO, *supra* note 43, § 36(2)(a).
292. ETO, *supra* note 43, § 36(2)(b).
293. ETO, *supra* note 43, § 36(2)(c).
294. Bahrain Legislative Decree No. 28, *supra* note 141, at art. 15. If the information is in clear language and is understandable, it may be sent by e-mail. This information is also available, on request, to relying third parties. *Id.*

3. Duty to Maintain Security Over the Private Key

A subscriber has a duty to exercise reasonable care in securing the private key that corresponds to the public key contained in the certificate.[295] The subscriber should do everything possible to ensure that the private key is not lost, stolen, or in the possession of an unauthorized person.[296] However, if the private key is lost or stolen, the subscriber should inform the CA at once[297] and the CA should immediately suspend the certificate containing the compromised private key.[298] During the suspension period, the subscriber's duty of reasonable care to secure the private key continues.[299]

4. Controller's Prerogative to Demand Deposit of the Private Key

The Controller may order a subscriber to turn over a private key for the following reasons:[300] (1) to prevent the commission of a legal offense;[301] (2) to "protect the sovereignty or integrity" of Nepal;[302] (3) to further "friendly relations with friendly countries;"[303] (4) to maintain "law and order;"[304] or as given by the Controller in his implementation regulations.[305] If the Controller issues such an order, the subscriber must immediately comply with it and deposit the private key with the Controller.[306] The Controller should not divulge any information about the deposited private key to unauthorized persons.[307]

M. E-Government

1. Electronic Publication of Government Notices Allowed

Any legal requirement that laws, regulations, executive orders or notices be published in Nepal's official newspaper, the *Gazette*, may also be fulfilled by publication in electronic form in the *Electronic*

295. ETO, *supra* note 43, § 37(1).
296. ETO, *supra* note 43, § 37(1).
297. ETO, *supra* note 43, § 37(2).
298. ETO, *supra* note 43, § 37(2).
299. ETO, *supra* note 43, § 37(3).
300. ETO, *supra* note 43, § 38.
301. ETO, *supra* note 43, § 38(1).
302. ETO, *supra* note 43, § 38(1).
303. ETO, *supra* note 43, § 38(1).
304. ETO, *supra* note 43, § 38(1).
305. ETO, *supra* note 43, § 38(1).
306. ETO, *supra* note 43, § 38(1).
307. ETO, *supra* note 43, § 38(2).

Gazette.[308]

2. Citizens Allowed to Make Electronic Filings, Retentions and Payments

Electronic documents may substitute paper documents whenever the law requires: (1) the filing of a form, application, or other document; (2) the generation or retention of a record; (3) the governmental issuance of a license, permit, approval or certificate; or (4) a record of payment of fees to the government.[309] Mere use of the electronic form in these cases will not be an acceptable ground for denial of the legal validity.[310]

3. Government May Accept Electronic Documents and Payments

If a prevailing law requires acceptance of documents and payments in paper form, the government may henceforth accept documents and payments in electronic form.[311] These electronic documents and payments have legal validity and this cannot be denied based on the mere fact of their electronic form.[312] Notwithstanding the above, a private person may not compel the government to accept a document or payment in electronic form and the government may not compel a private person to accept a document or payment in electronic form.[313]

Overall, Nepal's e-government provisions are commendable and better than most jurisdictions; many nations have no e-government provisions at all. E-government should be emphasized because it will lead to a reduction in cost and make governmental functions more convenient for citizens.[314] **Whenever it is practical and feasible, Nepal should make e-government mandatory instead of permissive, compelling certain governmental departments to: offer**

308. ETO, *supra* note 43, § 39(1).
309. ETO, *supra* note 43, § 39(2).
310. ETO, *supra* note 43, § 39(2).
311. ETO, *supra* note 43, § 40(1). The Controller will issue regulations concerning the "procedure, process and format" to be followed in submission of electronic documents. *Id.* § 40(3).
312. The government may issue specific procedures in this regard. ETO, *supra* note 43, § 40(3). For an article including a brief discussion of the length of time it may take to achieve the ETO's e-government initiatives, *see* Uttam Maharjan, *Cyber Act a Stepping Stone to ICT Development*, THE RISING NEPAL, May 21, 2005, at 1.
313. ETO, *supra* note 43, § 40(2).
314. In Hong Kong, for example, a substantial number of governmental services may now be accessed online, e.g., the scheduling of an interview for a visa or the scheduling of a wedding before a public official. *See* Blythe, *Hong Kong*, *supra* note 58.

online services; use and accept electronic signatures; accept documents and payments in electronic form; and issue documents and payments in electronic form. Finland has enacted a separate, more comprehensive e-government statute than Nepal, and it can be used as a model.[315]

4. Government's Digital Signatures

When the government requires a document issued or accepted, and if said document or record requires a signature, a digital signature may be used instead of a traditional ink signature.[316] The government will issue specific regulations for implementation of this provision.[317] Notwithstanding other security procedures mentioned in the ETO, the government may adopt a special security procedure pertaining to the utilization of digital signatures.[318]

N. Network Service Providers

Network service providers ("NSP") are "intermediaries"[319] which provide Internet or telecommunications services. NSP are responsible for the liabilities enumerated in the contracts with their subscribers.[320] They are also responsible for all liabilities listed in their license[321] and such other liabilities specified by the government.[322]

Notwithstanding the above, NSP are not, as a general rule, subject to any civil or criminal penalties merely because they have enabled subscribers to gain access to information or data of any third party.[323] However, NSP may be liable if they had knowledge that facts or

315. Finland's e-government statute facilitates the growth of electronic services for citizens by governmental departments, allows citizens to make required governmental filings or requests electronically, allows government to respond to those filings or requests electronically, and promotes achievement of security in electronic communication. It establishes detailed rules regarding the transmission of electronic messages, it authorizes governmental departments to use electronic signatures if the requirements of the ESA are complied with, and also allows governmental departments to effect service of its decisions upon citizens. Act on Electronic Services and Communication in the Public, 13/2003, at 1-2 (Fin.), *archived at* http://www.webcitation.org/5V5nTJZKI.

316. ETO, *supra* note 43, § 41(1).

317. ETO, *supra* note 43, § 41(3).

318. ETO, *supra* note 43, § 41(2).

319. ETO, *supra* note 43, § 42.

320. ETO, *supra* note 43, § 42(a).

321. ETO, *supra* note 43, § 42(b).

322. ETO, *supra* note 43, § 42(c).

323. ETO, *supra* note 43, § 43. The NSP must not have any control over the third party. Otherwise, the NSP may have liability. *Id.*

statements being disseminated by a third party are in violation of the ETO or its implementation regulations.[324]

The following should be added to the ETO: An intermediary should be required to: (1) have sufficient equipment and technical expertise commensurate with a trustworthy computer information system; and (2) be able to determine the exact time and place that an electronic message was sent and to securely store this information for at least six months.

O. Computer-Related Offenses and Punishments[325]

1. Tampering With Computer Source Documents

It is a crime to knowingly or intentionally conceal, destroy or alter (or intentionally or knowingly cause another to conceal, destroy or alter) any computer source code used for a computer, computer program, computer system or computer network, when the computer source code[326] is legally required to be retained for a specific duration.[327] The punishment for this crime is imprisonment (3 years maximum), or a fine (200,000 Rupees[328] maximum), or both.[329]

2. Obtaining Unauthorized Access to Computer Materials

It is a crime to use any program or data of a computer without authorization from its owner or rightful custodian.[330] Furthermore, it is also a crime if a user of a program or data has authorization from the owner or rightful custodian, but exceeds the scope of that authorization and obtains access to unauthorized materials.[331] The punishment will be

324. ETO, *supra* note 43, § 43; *see also* Ram Humagai, *Nepal: Landmark Cyber Law is Silent About Online Media*, NEPAL NEWS (Sept. 23, 2004), *archived at* http://www.webcitation.org/5VuDTcn0p (discussing the ETO's shortcomings, including its failure to regulate online news portals).

325. For a discussion of the problems that may possibly be incurred in trying to convert Nepal's police officers into "cyber cops," *see* Mahesh Singh Kathayat, *Cyber Crime Vs. Law Enforcement*, eKantipur.com (Nov. 22, 2004), *archived at* http://www.webcitation.org/5VJKRFiUA.

326. Computer source code is defined as "the listing of programmes, computer command, computer design and layout and programme analysis of the computer resource in any form." ETO, *supra* note 43, § 44.

327. ETO, *supra* note 43, § 44.

328. At the time of publication, one U.S. Dollar was equal to approximately sixty-four Nepal Rupees. [hereinafter Exchange Rate].

329. ETO, *supra* note 43, § 44.

330. ETO, *supra* note 43, § 45.

331. ETO, *supra* note 43, § 45.

a fine (200,000 Rupees[332] maximum) or imprisonment (3 years maximum), or both.[333]

3. Damaging a Computer or Information System

It is a crime to knowingly destroy, alter or incapacitate any part of a computer system or information system; this includes the hardware, software, data, networking, information programs, electronic records, and database.[334] It is also a crime to coerce, influence or entice another person to do so.[335] The punishment will be a fine (200,000 Rupees[336] maximum) or imprisonment (3 years maximum), or both.[337]

4. Electronic Publication of Illegal Materials

Publication on the Internet of materials deemed illegal under prevailing law is a crime.[338] It is also a crime to coerce, influence or entice another person into doing so.[339] The punishment will be a fine (100,000 Rupees[340] maximum) or imprisonment (five years maximum), or both.[341] Those committing subsequent offenses of this type will be given a punishment of 150 percent of the previous punishment.[342]

5. Dissemination of Private Information

It is a crime for a person to disseminate private information to an unauthorized person, even if the information was accessed and obtained with authorization.[343] This includes information from records, books, registers, correspondence, documents or other materials.[344] Depending upon the seriousness of the dissemination, the punishment will be a fine (100,000 Rupees[345] maximum) or imprisonment (2 years maximum), or both.[346]

332. *See* Exchange Rate, *supra* note 330.
333. ETO, *supra* note 43, § 45.
334. ETO, *supra* note 43, § 46.
335. ETO, *supra* note 43, § 46
336. *See* Exchange Rate, *supra* note 330.
337. ETO, *supra* note 43, § 46.
338. ETO, *supra* note 43, § 47(1).
339. ETO, *supra* note 43, § 47(1).
340. *See* Exchange Rate, *supra* note 330.
341. ETO, *supra* note 43, § 47(1).
342. ETO, *supra* note 43, § 47(2).
343. ETO, *supra* note 43, § 48.
344. ETO, *supra* note 43, § 48.
345. *See* Exchange Rate, *supra* note 330.
346. ETO, *supra* note 43, § 48.

6. Provision of False Information to a CA

It is a crime for a Digital Signature Certificate applicant to provide false information to a CA or the Controller.[347] The punishment will be a fine (100,000 Rupees[348] maximum) or imprisonment (2 years maximum), or both.[349]

7. Imposter CA's

It is a crime for an unlicensed CA to issue a Certificate.[350] The punishment will be a fine (100,000 Rupees[351] maximum) or imprisonment (2 years maximum), or both.[352]

It is a crime for an entity to publish a fake CA license or to make a false statement supporting a fake license, or to provide it to another person by any other means.[353] The punishment will be a fine (100,000 Rupees[354] maximum), provided that no certificate has been issued pursuant to the fake license.[355]

8. Publication of an Invalid Certificate

It is a crime for a person to publish an invalid certificate.[356] The offender must know that: (1) the CA listed on the certificate did not in fact issue the certificate; (2) the subscriber listed on the certificate has not accepted the certificate; or (3) the certificate has already been suspended or revoked (but, of course, it is not a crime to have published the certificate before it was suspended or revoked).[357] The punishment will be a fine (100,000 Rupees[358] maximum) or imprisonment (2 years maximum), or both.[359]

9. Failure to Submit Required Statements or Documents

347. ETO, *supra* note 43, § 49.
348. *See* Exchange Rate, *supra* note 330.
349. ETO, *supra* note 43, § 49.
350. ETO, *supra* note 43, § 50(1).
351. *See* Exchange Rate, *supra* note 330.
352. ETO, *supra* note 43, § 50(1).
353. ETO, *supra* note 43, § 50(2).
354. *See* Exchange Rate, *supra* note 330.
355. ETO, *supra* note 43, § 50(2).
356. ETO, *supra* note 43, § 50(3).
357. ETO, *supra* note 43, § 50(3).
358. *See* Exchange Rate, *supra* note 330.
359. ETO, *supra* note 43, § 50(3).

Where the ETO or its implementation regulations require a party to submit documents or statements to either the Controller or a CA within a prescribed time period, failure to do so is a crime.[360] The punishment will be a fine (50,000 Rupees[361] maximum).[362]

10. Failure to Maintain Records

If any party (e.g., a CA) is required to maintain records pursuant to the ETO or its implementation regulations, failure to do so is a crime.[363] The punishment will be a fine (50,000 Rupees[364] maximum).[365]

11. Forgery of a Digital Signature

It is a crime for a person to knowingly create, publish or provide a digital signature for the purpose of forgery or another illegal objective.[366] The punishment will be a fine (100,000 Rupees[367] maximum) or imprisonment (2 year maximum), or both.[368]

12. Abetment, Attempt and Conspiracy

An attempt to commit, to conspire to commit, or to abet another party to commit a computer crime is a crime.[369] The punishment will be according to the degree of the offense, and will be a fine (50,000 Rupees[370] maximum) or imprisonment (six months maximum), or both.[371]

It is also a crime to act as an accomplice, i.e., to assist the principal in the commission of a computer crime.[372] The punishment will be one-half the punishment meted out to the person who executed the computer crime.[373]

360. ETO, *supra* note 43, § 51(1).
361. *See* Exchange Rate, *supra* note 330.
362. ETO, *supra* note 43, § 51(1).
363. ETO, *supra* note 43, § 51(2).
364. *See* Exchange Rate, *supra* note 330.
365. ETO, *supra* note 43, § 51(2).
366. ETO, *supra* note 43, § 52.
367. *See* Exchange Rate, *supra* note 330.
368. ETO, *supra* note 43, § 52.
369. ETO, *supra* note 43, § 53.
370. *See* Exchange Rate, *supra* note 330.
371. ETO, *supra* note 43, § 53.
372. ETO, *supra* note 43, § 54.
373. ETO, *supra* note 43, § 54.

13. Right of Seizure

Law enforcement authorities in Nepal have the right to seize all computers and computer-related devices suspected to have been used in the commission of a computer crime listed in the ETO.[374]

14. Commission of Computer Crimes By Organizations

If an organization has committed a computer crime, the organization's chief executive officer shall be considered the violator.[375] If the chief executive officer is able to show that the crime occurred without his knowledge or that he attempted to prevent the crime, he shall not be liable;[376] If an officer of the organization (e.g., director, manager, secretary or other responsible person in the organization) was negligent, consented to the crime or had knowledge of it and acquiesced in the matter, then the organization and that responsible person will be liable.[377]

15. Default Punishment

If a person is involved in a computer crime listed in the ETO, but no punishment is specifically in the ETO, then the "default" punishment will be a fine (50,000 Rupees[378] maximum) or imprisonment (six months maximum), or both.[379]

16. "Double" Punishment Allowed

If any act listed as a computer crime under the ETO is also listed as a crime under another prevailing law, the ETO will not prevent the offender from adjudication and punishment under the other law.[380]

The list of computer crimes and punishments is a positive aspect of the ETO.

P. The Information Technology Tribunal

374. ETO, *supra* note 43, § 56.
375. ETO, *supra* note 43, § 57(1).
376. ETO, *supra* note 43, § 57(1).
377. ETO, *supra* note 43, § 57(2).
378. *See* Exchange Rate, *supra* note 330.
379. ETO, *supra* note 43, § 58.
380. ETO, *supra* note 43, § 59. Apparently, two penalties could be assessed for the same unlawful act.

1. The "Trial Court" of Cyber-Crimes

The Information Technology ("I.T.") Tribunal[381] is the forum of first-instance that will consider the computer crimes mentioned in Chapter 9 (Sections 44-59) of the ETO.[382] It was established by the government of Nepal by making an official notification in the *Nepal Gazette*.[383] It consists of three members: a lawyer, an I.T. person, and a business person.[384] The lawyer is the presiding officer.[385] Before beginning their duties, they must orally express their oath of office before the Chief Judge of the Appellate Court in a form and manner to be prescribed in the implementation regulations.[386] After the I.T. Tribunal renders its decision, a party may appeal the decision to the I.T. Appellate Tribunal within 35 days of the decision.[387]

2. Qualifications of the Members of the Tribunal

The lawyer must be qualified to serve as a judge of a District Court, or have experience as a judge of a District Court, and have knowledge of information technology.[388]

The I.T. person must be a citizen of Nepal, hold at least a masters degree in Computer Science or Information Technology, and have at least three years' experience in work pertaining to "electronic transactions, information technology or electronic communication."[389]

The business person must be a citizen of Nepal, hold at least a masters degree in management or commerce with a specialization in electronic transactions, and have three years' work experience in a related field.[390]

3. Tenure and Remuneration

381. I.T. Tribunal is defined as "the body established by § 60 of the ETO which is authorized to hear and decide e-commerce disputes in the first instance." ETO, *supra* note 43, § 2(l).
382. ETO, *supra* note 43, § 60(1). The Tribunal will exercise jurisdiction as prescribed by the Controller in the ETO's implementation regulations. ETO, *supra* note 43, § 60(3).
383. ETO, *supra* note 43, § 60(1).
384. ETO, *supra* note 43, § 60(1).
385. ETO, *supra* note 43, § 60(2).
386. ETO, *supra* note 43, § 62(3).
387. ETO, *supra* note 43, § 60(4).
388. ETO, *supra* note 43, § 61(1).
389. ETO, *supra* note 43, § 61(2).
390. ETO, *supra* note 43, § 61(3).

The tribunal members will have a five-year appointment, subject to renewal.[391]

Their remuneration and terms and conditions of service will be specified in the implementation regulations.[392]

The tribunal office will be considered vacant in the following situations: (1) at the end of the five year period, if no renewal has occurred; (2) when the tribunal member reaches the age of 63 years; (3) upon the death of the tribunal member; (4) upon the resignation of the tribunal member; (5) if the tribunal member is convicted of a crime of moral turpitude; or (6) whenever a governmental inquiry proves that the tribunal member has engaged in misbehavior or is incompetent.[393] However, in the governmental inquiry mentioned above, the tribunal member's right of due process will be recognized and he will be given a "reasonable opportunity" to defend himself."[394] Furthermore, the procedure to be followed in the inquiry will be specified in the ETO's implementation regulations.[395]

If a vacancy arises, the government will appoint a replacement from among those possessing the qualifications specified in section sixty-one of the ETO. The replacement will serve out the remainder of the unexpired term.[396]

The I.T. Tribunal will be provided an administrative staff as necessary to carry out its functions.[397] Details will be covered in the implementation regulations.[398] In prosecuting the cases appearing before it, the I.T. Tribunal must follow the procedures specified in the implementation regulations.[399]

Q. The I.T. Appellate Tribunal

1. The "Appellate Court" of Cyber-Crimes

By notification in the *Nepal Gazette*, the government also established the Information Technology Appellate Tribunal.[400] The Tribunal is

391. ETO, *supra* note 43, § 62(1).
392. ETO, *supra* note 43, § 62(2).
393. ETO, *supra* note 43, § 63(1). In the case of item no. 6, this inquiry will proceed according to the rules prescribed in the implementation regulations. ETO, *supra* note 43, § 63(3).
394. ETO, *supra* note 43, § 63(1).
395. ETO, *supra* note 43, § 63(3).
396. ETO, *supra* note 43, § 63(4).
397. ETO, *supra* note 43, § 64(1).
398. ETO, *supra* note 43, § 64(2).
399. ETO, *supra* note 43, § 65.
400. ETO, *supra* note 43, § 66(1). Appellate Tribunal is defined as the body

empowered to consider appeals of the orders or decisions made by the I.T. Tribunal, the Controller, or a CA.[401] This body will also consist of three members: a lawyer, an I.T. person, and a business person.[402] As with the I.T. Tribunal, the lawyer is the presiding officer.[403] Before commencing their duties, they are required to take an oath of office in the presence of the Chief Justice of the Supreme Court.[404]

2. Qualifications of the Members of the I.T. Appellate Tribunal

The lawyer must be qualified to serve as a Judge of the Appellate Court, or have experience as a Judge of the Appellate Court. Furthermore, the lawyer must have a general knowledge of the information technology field.[405]

The I.T. person must be a citizen of Nepal holding at least a masters degree in Computer Science or Information Technology. This person must have a minimum of five years' experience in electronic transactions, information technology or electronic communication.[406]

The business person must be a citizen of Nepal holding a graduate degree in management or commerce with a specialization in electronic transactions. This person must also have at least five years' experience in a relevant field.[407]

3. Terms and Remuneration

The I.T. Appellate Tribunal members will serve for a term of five years, subject to reappointment.[408] Remuneration and other terms and conditions of office will be specified in the ETO's implementation regulations.[409]

The I.T. Appellate Tribunal positions will be considered vacant in the following situations: (1) when the five-year term has expired, and no

established by § 66 of the ETO which is authorized to consider appeals of decisions made by Tribunals. *Id*. § 2(q).

401. ETO, *supra* note 43, § 66(1). Rules pertaining to exercise of the Appellate Tribunal's jurisdiction will be issued by the Controller in the ETO's implementation regulations. *Id*. § 14.

402. ETO, *supra* note 43, § 66(1).

403. ETO, *supra* note 43, § 66(2).

404. ETO, *supra* note 43, § 68(3).

405. ETO, *supra* note 43, § 67(1)

406. ETO, *supra* note 43, § 67(2).

407. ETO, *supra* note 43, § 67(3).

408. ETO, *supra* note 43, § 68(1).

409. ETO, *supra* note 43, § 68(2).

renewal has occurred; (2) upon the member's reaching the age of 63 years; (3) upon the death of the member; (4) upon the resignation of the member; (5) if convicted of a crime of moral turpitude; and (6) if a governmental inquiry proves that the member has engaged in misbehavior or is incompetent.[410] However, in the governmental inquiry mentioned above, the member's right of due process will be recognized and he will be given a "reasonable opportunity" to defend himself.[411] The procedure to be followed will be prescribed in the ETO's implementation regulations.[412]

If a vacancy arises in the I.T. Appellate Tribunal membership, the government will appoint a replacement possessing the qualifications laid out in Section 67 of the ETO to serve out the unexpired term.[413]

The I.T. Appellate Tribunal will be assigned an administrative staff to provide assistance in carrying out its duties.[414] The ETO's implementation regulations will provide details pertaining to the administrative staff.[415]

The procedures to be followed by the I.T. Appellate Tribunal in the consideration of the cases appearing before it will be issued by the Controller in the ETO's implementation regulations.[416]

Nepal's utilization of a panel of experts in the I.T. Tribunal and the I.T. Appellate Tribunal appears to be a good idea that merits further research. Its neighbor, India,[417] which established a special Adjudicating Officer to consider e-commerce cases in the first instance, and a Cyber Regulations Appellate Tribunal at the next level, may have influenced Nepal. However, Nepal's scheme may prove better because it employs a 3-person tribunal at both the first-instance forum and the appellate forum, where India uses only one Adjudicating Officer in the first-instance forum. Furthermore, India does not specifically prescribe the legal, business and I.T. expertise required by the Adjudication Officer and the members of the Cyber Regulations Appellate Tribunal as Nepal's ETO does.

R. Legal Proceedings Under the ETO

410. ETO, *supra* note 43, § 69(1).
411. ETO, *supra* note 43, § 69(1).
412. ETO, *supra* note 43, § 69(3).
413. ETO, *supra* note 43, § 69(4).
414. ETO, *supra* note 43, § 70(1).
415. ETO, *supra* note 43, § 70(2).
416. ETO, *supra* note 43, § 71.
417. Information Technology Act, *supra* note 200, §§ 46-8, 57. Another similarity between Nepal and India is that both of their statutes are first-generation; the digital signature is the only type of electronic signature that is legally recognized.

Complaints based upon alleged violations of the ETO must be filed within thirty-five (35) days of the receipt of information pertaining to those allegations.[418] In all legal proceedings brought under the ETO, only the government shall be allowed to be the complainant.[419] The Controller will cooperate with the police in the investigation of any alleged violations of the ETO.[420] If a defendant is found to be in violation of the ETO, that person or entity must indemnify the party that has incurred a financial loss.[421]

S. Implementation Regulations

The government reserves the right to issue implementation orders and directives applicable to the Controller or to a CA. If they are issued, they must be complied with.[422] Furthermore, the government may issue rules, regulations and directives applicable to all concerned parties deemed necessary to implement the ETO.[423]

VI. Other Recommended Additions to the ETO

A. Consumer Protections Needed in E-Contracts

Consumer protections in e-commerce are needed. As a model of good consumer protections, Nepal can look to Tunisia's computer law.[424] Tunisia's law provides (1) a "last chance" for buyers 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) the right to a refund if the goods are late or if they do not conform to the specifications; and (4) the risk remains on the seller during the 10-day trial period after the goods have been received. Tunisian cyber-buyers enjoy some of the best protections in the world.[425]

418. ETO, *supra* note 43, § 74.
419. ETO, *supra* note 43, § 75(1). The cases will be considered to be part of Schedule I of the State Cases Act of 1992. *Id.*
420. ETO, *supra* note 43, § 75(2).
421. ETO, *supra* note 43, § 76.
422. ETO, *supra* note 43, § 73.
423. ETO, *supra* note 43, §§ 78-79.
424. Electronic Exchanges and Electronic Commerce Law, Law No. 83 of 2000, art. 25-37, (2000) (Tunis.), *translated in* 16 ARAB LAW QUARTERLY 4 (2001); s*ee also* Blythe, *Critique*, *supra* note 96.
425. Korea is one of the few nations that may offer better consumer protections than Tunisia. That country has enacted a separate statute specifically for e-commerce consumer protections—the E-Commerce Transactions Consumer

B. Promote "Cybersuites"

Economically underdeveloped nations such as Nepal need to be on the lookout for new sources of revenue. Accordingly, Nepal should consider the promotion of "cybersuites" as exemplified in the Republic of Vanuatu. Vanuatu enacted its e-Business Act ("EBA") to regulate e-commerce websites that have been rented by international business firms looking for a tax haven.[426] The EBA creates an Internet Free Trade Zone where individuals and firms can consummate e-commerce transactions while taking advantage of Vanuatu's low business income tax rates. Vanuatu-based websites—referred to as "cybersuites" in the EBA—are rented to foreign parties so that they may engage in e-commerce without the necessity of establishment of a formal international corporation with directors, shareholders and a registered office. Cybersuite proprietors are provided assistance in the creation of the website and its maintenance.[427]

C. Special Rules for Carriage Contracts

Because of the special requirements pertinent to contracts for the delivery of goods, or "carriage" contracts, some jurisdictions have adopted special rules. In consideration of this possibility, Nepal can

Protection Act. *See* Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions, STATUTES OF THE REPUBLIC OF KOREA, Vol. 13, pp. 481 to 485-30 [hereinafter "CPA"]. Originally enacted by Law No. 6687 (March 30, 2002), and amended by Act Nos. 7315 and 7344 of 31 December 2004 and 27 January 2005, respectively. Furthermore, the CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of 31 March 2005; these amendments became effective on 1 April 2006. For a thorough analysis of the CPA, *see* Blythe, *Korea*, *supra* note 109. Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. Electronic Commerce Law of 7 Jan. 2004, art. 37 and 38 (Iran), *archived at* http://www.webcitation.org/5V5qLCMAr. *See also* Blythe, *Tehran*, *supra* note 108.

426. E-Business Act, Act No. 25 of 2000), Preamble (2000) (Vanuatu), *archived at* http://www.webcitation.org/5VJLIOyol. For a discussion of the E-Business Act by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—*see* Hon. Prime Minister Barak T. Sope Maautamate, MP, The E-Business Act of 2000, The International Companies (E-Commerce Amendment) Act of 2000, The Companies (E-Commerce Amendment) Act of 2000: A Plain English Explanation, pp. 8-10 (Vanuatu); *archived at* http://www.webcitation.org/5VuE8co51. *See also* Blythe, *South Pacific*, *supra* note 104.

427. Lowtax.net, *Vanuatu: E-commerce*, *archived at* http://www.webcitation.org/5VuDXr7Na.

look to the e-commerce law of Colombia,[428] Canada,[429] Singapore[430] and Bahrain[431] for examples.

D. Add Domain Name Registration

To consolidate Nepal's computer law in a central location, domain name registration should be added as a new section of the ETO.[432]

E. Add Rules Relating to E-Notes and E-Funds Transfers

In an innovative move, Jordan decided to include rules pertinent to the transfer of electronic notes and electronic funds transfers in its Electronic Transactions Law ("ETL"). Electronic notes are transferable if all requirements for "negotiable instruments" under the Jordanian Commercial Code are complied with, and if the drawer of the note agrees that it is negotiable. Electronic funds transfers are sanctioned by the ETL as well. However, the participating financial institution must

428. Colombia's statute contains rules regarding these and other aspects of a carriage contract: (1) detailed description of the goods; (2) issuance of receipt; (3) confirmation of shipment; (4) notification of terms of the contract; (5) instructions to be conveyed to the transporter; (6) request of delivery of the goods; (7) authorization to deliver the goods; (7) buyer's notification of loss or damage of goods during transit; (8) seller's promise to deliver the goods to buyer or her agent; and (9) acquisition, waiver or transfer of rights in the agreement. In Colombia, e-documents may be used in the creation or implementation of carriage contracts, notwithstanding the fact that another statute may mandate the utilization of paper documents. This applies regardless of whether the statute creates a legal requirement, or provides for detrimental consequences if paper documents are not used. However, in order for e-documents to be used in the transfer of a right or obligation under a carriage contract, a "reliable method" must be employed to ensure the security and integrity of the message. Once data messages have begun to be used, paper documents are no longer valid. A party cannot revert to the use of paper documents until the other party has been informed that, henceforth, paper documents are to be used instead of data messages. Reversion to paper documents will not affect the rights of the parties which were created with e-documents. If a legal regulation exists in reference to paper documents relating to a carriage contract, that regulation will also be applied to a digital message used *in lieu* of paper documents. This Bill Defines and Regulates the Access and Use of Data Messages, Electronic Trade and Digital Signatures, and Establishes the Certification Entities, and Set Forth Some Other Provisions, Law 527, arts. 26-27 (1999) (Colom.), *translated in* Official Translation No. 7 (Ministry of Justice, 1999), *archived at* http://www.webcitation.org/5VuDcGcVw.

429. Uniform Electronic Commerce Act, §§ 24-25 (Canada 1999), *archived at* http://www.webcitation.org/5VJLkbz2x.

430. Blythe, *Singapore*, *supra* note 101.

431. Bahrain Legislative Decree No. 28, *supra* note 141.

432. For example, the Kingdom of Bahrain has incorporated domain name registration as part of its Electronic Transactions Law. Bahrain Legislative Decree No. 28, *supra* note 141, at art. 21.

do everything reasonably necessary to ensure the security of the transfer and to maintain the confidentiality of the customer's private information.[433]

VII. Summary and Conclusions

A. Nepal's Electronic Transactions Ordinance

In order to promote its nascent cyber-trade, the government of Nepal enacted an e-commerce law in 2004—the Electronic Transactions Ordinance ("ETO"). The ETO provides a basic framework for attainment of secure and reliable e-commerce transactions. The ETO is technologically-specific, requiring the utilization of the digital signature (and its related public-key-infrastructure) because it provides a relatively higher degree of security than other electronic signatures.

Under the ETO, private parties are not mandated to use e-documents, but they may elect to do that if all parties to a transaction are in agreement. E-documents are deemed to be authentic if they have a digital signature affixed to them, and they cannot be disavowed merely because they are in electronic form. If a statute requires the retention of a document, ordinarily it may be stored in electronic form. If another statute requires the affixation of an ink signature on paper, the ETO ordinarily allows a digital signature affixed to an e-document to comply with that requirement. Finally, e-documents are sufficient to comply with a statutory requirement for an original document to be produced, provided the electronic document: (1) is accessible; (2) is capable of being reproduced in the same format it was in originally; and (3) exhibits details of time and place in which the document was sent and received.

Certifying authorities ("CA") issue certificates to verify the authenticity and the integrity of the digital signatures which are issued to their subscribers. The ETO establishes the Office of the Controller to license and oversee the CA's operational activities. The Controller is given a substantial amount of authority in this regard and is empowered to issue CA Regulations which must be adhered to by the CA's. The CA's license may be suspended or revoked by the Controller. Although other nations often fail to address the issue of a bankrupt CA, Nepal does consider that issue and includes bankruptcy as a ground for revocation of a CA's license, an idea which deserves to be considered by other nations. The ETO also lists grounds for the suspension or

433. Electric Transactions Law, Law No. 85 of 2001, arts. 19-27 (2001) (Jordan), *archived at* http://www.webcitation.org/5V5r5iRuK.

revocation of the certificates which have been issued by the CA. The ETO mandates the Controller to conduct an annual audit of every CA, and any irregularities must be promptly rectified by the CA. The Controller also has the authority to conduct an on-site inspection of the CA. Unlike some other jurisdictions, Nepal has a compulsory CA system, i.e., all CA's must have a license that has been issued by the Controller.

The ETO contains a provision allowing for the government to recognize foreign CA's. If recognition is given to a foreign CA, it will be allowed to issue certificates pursuant to the ETO within Nepal just as if it was a domestic entity. This provision is necessary because e-commerce is an inherently international phenomenon, it knows no borders, and it is essential to have recognition of CA's of foreign nations in order to provide a reliable and secure foundation for e-commerce on a worldwide basis.

The ETO contains basic e-government rules. It allows government decrees and notices to be published in electronic form. Government agencies may accept documents in electronic form and the government may employ a digital signature to authenticate official documents.

Network Service Providers ("NSP")—intermediary entities providing internet service to the consumer—are also covered in the ETO. They are subject to potential liabilities enumerated in their license which is issued by the government, and in the contracts they make with their consumer-subscribers. In order to promote free speech over the internet, NSP's will ordinarily not be held liable for the information they disseminate over the internet if it was created by other parties.

One of the most impressive sections of the ETO concerns computer crimes. This section thoroughly deals with criminal acts relating to the computer. It prohibits: (1) alteration of computer source code; (2) unauthorized access to computer materials; (3) damaging computer equipment; (4) publication of illegal materials using computers; (5) dissemination of confidential information gleaned from a computer; (6) giving false information to a CA in an application for a certificate; (7) imposter CA's; (8) failure of the CA to submit required statements or documents to the Controller; and (8) computer fraud. Specific criminal penalties are provided for the various infractions. Interestingly, the ETO also established "long arm" jurisdiction; the criminal crimes section purportedly applies to anyone committing the stated offenses affecting computers based in Nepal, even if the criminal is a foreign party residing outside the borders of Nepal. Also, realizing the need for technical expertise in dealing with computer crimes, the ETO established two special courts: the Information Technology ("I.T.) Tribunal, the court of first instance; and the I.T. Appellate Tribunal to hear appeals from the

I.T. Tribunal. Establishment of "computer courts" is a clever addition to the ETO, another idea which deserves to be considered by other nations.

Nepal has crafted a satisfactory initial e-commerce law. It is one that other nations should study, especially with respect to: (1) the specification of computer crimes and the related penalties; (2) the establishment of special I.T. courts to prosecute computer crimes; (3) the assertion of "long arm" jurisdiction over foreigners committing offenses through computers located within Nepal; and (4) bankrupt status as a ground for revocation of a CA's license.

B. Tweaking the ETO

Although it was an adequate first step, the ETO needs to be fine-tuned. The following provisions should be added to Nepal's e-commerce law, or amendments should be made to the existing law: (1) adoption of an inclusive definition of an e-signature and recognition of many types of e-signatures, while continuing to give the digital signature most-favored-status; (2) distinguish the owner and subscriber of an e-document when the owner uses an agent; (3) a rule concerning admissibility and weight of evidence of e-documents; (4) more specific requirements for the applicability of the legal presumption of authenticity of e-documents and e-signatures; (5) reduce the number of exclusions from coverage; (6) allow use of e-documents to meet statutory requirements of delivery and notarisation; (7) a rule concerning whether a sender may assume his message was correctly received by the addressee; (8) a rule dealing with the sending of duplicate e-messages; (9) a rule pertinent to assumed time of dispatch when the sender and receiver use the same computer; (10) financial resources required by a CA; (11) required contents of a CA's certification practice statement; (12) CA's written notice to subscriber before issuance of certificate; (13) intermediary's record-keeping requirements; (14) consumer protections; (15) tax-haven "cybersuites" as a new source of government revenue; (16) special rules for carriage contracts, (17) domain name registration; and (18) rules relating to e-notes and e-funds transfers.