A CRITIQUE OF INDIA'S INFORMATION TECHNOLOGY ACT AND RECOMMENDATIONS FOR IMPROVEMENT

Stephen E. Blythe*

ABSTRACT

India's Information Technology Act (ITA) recognizes the legal validity of E-documents, E-signatures and E-contracts, and also promotes E-government. E-documents are not allowed in wills, trusts, sales of real property, negotiable instruments and powers-of-attorney. An E-document may be used to satisfy a statutory requirement of: writing; authentication; retention; publication; and governmental filing, issuance or payment. A digital signature complies with a statutory requirement for a handwritten signature to be affixed on paper. The ITA includes E-contract rules relating to: attribution, acknowledgement of receipt, and time and place of transmission and reception of an electronic message. Rules are provided for the regulation of Certification Authorities (CA) and third parties whose duty is to vouch for the authenticity and integrity of an electronic message that has been signed with a digital signature. Those rules are implemented by the Controller. India has adopted a compulsory system of CA licensing; no party may offer certification services without a license. A CA is mandated to: publicly display its license; issue certificates to successful applicants; and manage outstanding certificates by keeping the information in them current, and suspending or revoking them if they contain inaccuracies. A CA's license may be suspended or revoked for good cause shown. Subscribers are responsible for ensuring that all information given to the CA is accurate and that all information contained in the certificate is correct. Ordinarily, network service providers have limited liability. The ITA includes civil and criminal

---

* Professor of Law & Accounting, School of Management, New York Institute of Technology, Manama, Kingdom of Bahrain. Ph.D. Candidate (Law), The University of Hong Kong (China); Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law), University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. He practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance-defense litigation) in Oklahoma City, and has engaged in management consulting in 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.

offenses and related penalties. The Controller appoints adjudicating officers to hear both civil and criminal cases relating to the ITA and to render decisions accordingly. Appeal may be taken to the Cyber Regulations Appellate Tribunal and eventually to the High Court. The federal government of India and the Controller are empowered to issue regulations necessary for implementation of the ITA.

OBJECTIVES OF THE ARTICLE

The objectives of this article are to: (1) introduce the reader to India's economy and E-commerce activity; (2) explain the role of electronic signatures; (3) explain the role of the evolution of electronic signature law; (4) analyze India's Information Technology Act (ITA); and (5) make recommendations for improvement of that statute.

I. INDIA'S ECONOMY AND E-COMMERCE

Two-thirds of India's 1.1 billion citizens depend upon agriculture for their income. However, India's economic growth is driven by other sectors of the economy: textiles, chemicals, steel, transportation equipment, cement, mining, petroleum, machinery and software. Since 1994, India's economy has achieved admirable growth at an average annual rate of 6.8%. However, governmental controls on foreign trade and investment have had a negative effect on economic development; in 2004, tariffs on imported goods averaged 20%. Furthermore, privatization of government-owned firms has been slow. The government has pledged to adopt incentives to encourage more investment in India's insurance, telecommunications and civil aviation industries.[1]

The people of India are simultaneously its primary resource and its disadvantage. India has a large number of well-educated English-speaking persons able to contribute to multinational firms, such as those in the software industry. However, the country must deal with the problem of a large and growing population. India has 15% of the world's people, yet occupies only 2.4% of the world's land. Despite the impressive growth rate of the economy, the income of 25% of India's citizens is below the poverty line.[2]

---

1. U.S. CENT. INTELLIGENCE AGENCY, THE WORLD FACTBOOK, *India* 258-259 (2005), *available at* http://www.cia.gov/cia/publications/factbook/geos/in.html (last visited Oct. 23, 2006).

2. U.S. DEP'T OF STATE, BUREAU OF SOUTH AND CENTRAL ASIAN AFFAIRS, *Background Note: India* (2005), *available at* http://www.state.gov/r/pa/ei/bgn/3454.htm (last visited Oct. 23, 2006).

Although E-commerce has great potential in India, to date the potential has been unrealized due to the low percentage of Indians with internet connections. Less than 20 million persons in India (in a population of 1.1 billion) had internet access in 2003, but 50 million Indians were using the internet by 2005.[3] India's new middle class—the group expected to participate most in E-commerce—is comprised of about 300 million citizens. Significantly, this is equal to the total number of U.S. consumers. The growing strength and size of the Indian middle class bodes well for the proliferation and prosperity of Indian E-commerce. E-commerce transactions were estimated to be in excess of $40 billion in 2005,[4] and were expected to reach $100 billion by 2008.[5]

II. ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[6] 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 an intent to authenticate a writing,"[7] 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."[8] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[9]

A well-known U.S. consumer group has stated, "[g]iven the

---

3. U.S. CENT. INTELLIGENCE AGENCY, *supra* note 1, at 259.

4. Puneet Mehrotra, *E-commerce 2004 – Good News Ahead*, Cyberzest.com, http://www.punit.cyberzest.com/index.php?id=650ffe0fe3 (last visited Oct. 23, 2006).

5. GatewayforIndian.com, E-commerce in India, http://www.gatewayforindia.com/technology/e-commerce.html (last visited Oct 23, 2006).

6. *See, e.g.*, U.C.C. §§ 2-201, 2-209 (2005).

7. Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of Law and Legislation*, 564 PLI/Pat 125, 162 (1999).

8. Council Directive 1999/93, art. 2, 2000 O.J. (L13) 14 (EC). Indian law has no definition of an electronic signature. However, it defines "electronic form" as "any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device." ITA, *infra* note 76, § 2(1)(r). An "electronic record" is defined as a "date, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro device." *Id.* § (2)(1)(t).

9. 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).

current state of authentication technology, it's much easier to forge or steal an e-signature than a written one."[10] This statement seems to assume that all E-signatures offer an equal degree of security. However, such an assumption would be erroneous; some electronic signatures offer more security than others. It is prudent for E-commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

A. Online Contracts: Four Levels of Security

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

1. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[11]

2. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased.[12]

3. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently difficult to replicate by a would-be cyber-thief. Examples include: a voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, a digital reproduction of a fingerprint,[13] 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.[14] For example, if a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an

---

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

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

12. *Id.*

13. *Id.* With the highly successful Hon Kong Identity Card, the two thumb prints are used as a biometric identifier. *See* Rina C.Y. Chung, *Hong Kong's "Smart" Identity Card: Date Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PAC. L. & POL'Y J. 518 (2003).

14. Stern, *supra* note 11, at 395-96. *See also* Cyber-Sign.com, The Legality of Electronic Signatures Using Cyber-Sign is Well Established, http://www.cybersign.com/com/news_news.htm#Top (last visited Oct. 25, 2006).

imposter.[15]

Biometrics, despite its potential utility as a form of electronic signature, has at least two drawbacks in comparison with the digital signature: (1) the attachment of a person's biological traits to a document does not ensure that the document has not been altered, i.e., it "does not freeze the contents of the document;"[16] 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.[17] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[18] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[19]

4. The digital signature is considered the fourth level because it is more complex than biometrics.[20] Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document.[21] It is "the sequence of bits

---

15. Cyber-sign.com, *supra* note 14.

16. K.H. Pun et al., *Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?,* 32 HONG KONG L.J. 241, 256 (2002).

17. *Id.* at 257.

18. *See id.* However, one of the experts in computer law and technology, Benjamin Wright, is a notable exception. Wright contends that biometrics is a more preferable authentication method in the case of the general public, although he concedes that digital signatures using PKI (discussed below) 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 one "basket," and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public would be sharing the risk with other parties involved in the transaction, and the need to protect the "private key" is not so compelling. *See* Benjamin Wright, *Eggs in Basket: Distributing the Risks of Electronic Signatures,"* 32 UWLA L. REV. 215, 225-26 (2001).

19. *See* Chung, *supra* note 13.

20. Under Indian law, a digital signature is defined as "authentication of any electronic record by a subscriber by means of an electronic record or procedure in accordance with the provisions of [the Information Technology Act] section 3." ITA, *infra* note 76, § 2(1)(p). A subscriber is defined as "a person in whose name the Digital Signature Certificate is issued." *Id.* § 2(1)(zg).

21. 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." Electronic Transactions Ordinance, (2004) Cap. 553, § 2(1)

that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key."[22] 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.[23]

B. Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure, or PKI.[24] PKI consists of four steps:

1. The first step in utilizing this technology is to create a public-private key pair.[25] The private key[26] will be kept in confidence by the sender,[27] but the public key[28] will be available online.[29]

2. The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it.[30] A "hash value" is created by applying a "hash function"—a standard mathematical function—to the contents of the electronic document.[31]

(H.K.).

22. Smedinghoff, *supra* note 7, at 146.

23. Christopher T. Poggi, *Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation*, 41 VA. J. INT'L L. 224, 250-251 (2000).

24. Susanna Frederick Fischer, *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).

25. The two keys must be uniquely identified as belonging to the subscriber. Together, they are considered to be a "functioning key pair." ITA, *infra* note 76, § 3(4).

26. Under Indian law, a private key is defined as "the key of a key pair used to create a digital signature." *Id.* § 2(1)(zc).

27. *PKI Assessment Guidelines*, 2001 A.B.A. SEC. SCI. & TECH. L. 301 (PAG v. 0.30, Public Draft for Comment No. 25), *available at* http://www.abanet.org/scitech/ec/isc/pagv30.pdf (last visited Oct. 25, 2006) [hereinafter ABA].

28. Indian law defines a public key as "the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate." ITA, *infra* note 76, § 2(1)(zd).

29. *See* ABA, *supra* note 27, at 305. Indian law defines a "key pair" used in an asymmetric crypto system as "a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key." ITA, *infra* note 76, § 2(1)(x).

30. *See* ABA, *supra* note 27, at 305.

31. *See* ITA, *infra* note 76, § 3(2). Under Indian law, a hash function is described as "an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as 'hash result' such that an electronic record yields the same hash result every time the algorithm is executed with same electronic record as its input making it computationally infeasible—(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm; [and] (b) that two electronic records can produce

The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Whereupon, the hash function is encrypted, or scrambled, by the signatory using his private key.[32] "The encrypted hash [function] is the 'digital signature' for the electronic document."[33]

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

4. The fourth step is for the recipient to decrypt the digital signature using the sender's public key.[34] If decryption is possible the recipient knows the message is authentic, i.e., that it came from the purported sender. Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest.[35] If they match, the recipient knows the message has not been altered.[36]

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. Furthermore, the encryption of the hash value with the signatory's private key uniquely links "the digital signature to the signatory, [i.e.] the owner of the private key."[37] Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific."[38]

The digital signature is the only form of electronic signature which

---

the same hash result using that algorithm." *Id.*

32. *See id.* § 3. For an electronic record to be properly authenticated under Indian law, asymmetric encryption must have been used in conjunction with a hash function to "envelope and transform the initial electronic record into another electronic record." *Id.* § 3(2). Asymmetric encryption provides one of the highest—if not *the* highest—degree of security in electronic transactions. Indian law defines an asymmetric crypto system as "a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature." *Id.* § 2(1)(f).

33. Pun et. al., *supra* note 16, at 249.

34. *Id.* Anyone should be able to confirm the authenticity of the subscriber, and the integrity of the electronic document the subscriber's digital signature is attached to, using the publicly-accessible public key of the subscriber. ITA, *infra* note 76, § 3(3).

35. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, 1996 ABA SEC. SCI. & TECH. L., *available at* http//:www.abanet.org/ftp/pub/scitech/ds-ms.doc (last visited Oct. 24, 2006) [hereinafter Information Security Committee].

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

37. Pun et. al., *supra* note 16, at 250.

38. *Id.*

satisfies all three of the United Nations Commission on International Trade Law (UNCITRAL) security evaluation factors, i.e., that an electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud. [39] Verification is achieved because the digital signature will accompany the document, allowing for confirmation of the identity of the signatory.[40] Approval is attained via computation of the hash value of the electronic document, which freezes the contents of the document at the time of creation of the digital signature. 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.[41]

D. Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. First, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common in most other forms of electronic signatures. The password and PIN face similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized.[42]

The second disadvantage of the digital signature pertains to the certificate,[43] which must be issued by a Certification Authority (CA).[44]

---

39. *Id.* at 256. Under Indian law, a secure computer information system is defined as "computer hardware, software, and procedure that– (a) are reasonably secure from [unauthorized] access and misuse; (b) provide a reasonable level of reliability and correct operation; (c) are reasonably suited to performing the intended functions; and (d) adhere to generally accepted security procedures." ITA, *infra* note 76, § 2(1)(ze). "Security procedure" refers to "the security procedure prescribed under [the Information Technology Act] in section 16 by the Central Government." *Id.* § 2(1)(zf). Section 16 of the ITA is discussed in detail below.

40. Pun et. al., *supra* note 16, at 252. Indian law defines verification (in reference to digital signatures, electronic records, and public keys) as the determination of whether: "(a) the initial electronic record was affixed with the digital signature by the use of [a] private key corresponding to the public key of the subscriber; [and] the initial electronic record is retained intact or has been altered since such electronic record was so fixed with the digital signature." ITA, *infra* note 76, § 2(1)(zh).

41. Pun et. al., *supra* note 16, at 252.

42. *Id.* at 253.

43. Indian law refers to a "certificate" as a "Digital Signature Certificate" and defines it as "a Digital Signature Certificate issued under [the Information Technology Act] subsection (4) of section 35." ITA, *infra* note 76, § 2(1)(q). Section 35(4) of the ITA is

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.[45] Because the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

E. The Critical Role of the Certification Authority

In order for PKI to realize its potential, it is crucial that the user be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If A (the sender) and B (the receiver) are attempting to consummate an online transaction, B needs an independent confirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that an imposter could have sent B the public key, contending that it belongs to A when in fact it does not. Accordingly, a reliable third party—the Certification Authority—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[46]

The most important job of the CA is to issue certificates which confirm basic facts about the subscriber, the subject of the digital certificate. The certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties: the name and address of the CA that issued the certificate; the name, address and other attributes of the subscriber; the subscriber's public key; and the digital signature of the CA.[47] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[48]

---

discussed in detail below.

44. The issuers of Certificates are referred to as Certification Authorities ("CA") in this article because that is a more generally accepted international term. Indian law uses the term "*Certifying* Authority." In India, a Certifying Authority is defined as "a person who has been granted a [license] to issue a Digital Signature Certificate under [the Information Technology Act] section 24." ITA, *infra* note 76, § 2(1)(g). A "license" refers to a "[license] granted to a Certifying Authority under [the Information Technology Act] section 24." *Id.*, §2(1)(z). Section 24 of the ITA is discussed in detail below.

45. Pun et. al., *supra* note 16, at 253.

46. 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).

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

48. Hogan, *supra* note 46, at 425-426.

In making an application to a CA for a certificate, the prospective subscriber must provide some sort of photo I.D., e.g., a passport or a driver's license. If the application is approved and the certificate is issued, the CA will issue a private key to its new subscriber which corresponds to the public key. This is done, however, without disclosing the specifics of the private key.[49] The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered by the CA. Ordinarily, however, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued.[50]

In order to indicate the authenticity of the digital certificate, the CA will sign it with his digital signature. Typically, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties in need of communication with the subscriber. Additionally, the online repository contains information pertaining to digital certificates which have been revoked or suspended by the CA due to lost or expired private keys. This is an important positive aspect of PKI technology. The general public has access to the status of digital signatures and relying third parties are kept informed, allowing them to judge whether they should place reliance on communications signed with a certain private key.[51]

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber. 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.[52]

A certificate is only as reputable as the CA that issues it. If the CA is unreliable and untrustworthy, the certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate.[53]

---

49. Smedinghoff, supra note 7, at 149.

50. *Id.* at 150.

51. Hogan, *supra* note 46, at 427.

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

53. David Hallerman, *Will Banks Become E-Commerce Authorities?,* BANK TECH. NEWS, June 1, 1999.

III. ELECTRONIC SIGNATURE LAWS

A. *The First Wave: Technological Exclusivity*

In 1995, the U.S. state of Utah became the first jurisdiction in the world to enact an electronic signature law.[54] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[55] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature include Germany, Italy, Malaysia, Russia and India.[56]

Unfortunately, these jurisdictions' choice of "technological-exclusivity" is burdensome and overly-restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's disadvantages: more expense, lesser convenience, more complication and less adaptability to technologies used in other nations, or even by other persons within the same country.[57]

B. *The Second Wave: Technological Neutrality*

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

54. *See* UTAH CODE ANN. §§ 46-3-101 thru 504 (1999). The Utah Digital Signatures Act was, however, repealed in 2006. Press Release, Jon Hutsman, Jr., Governor, State of Utah, Governor Signs 103 Bills and 2 Resolutions (March 10, 2006), *available at* http://www.utah.gov/governor/news/2006/news_03_10_06.html (last visited Nov. 8, 2006).

55. *See* UTAH CODE ANN. §§ 46-3-101 thru 504 (1999).

56. Chung, *supra* note 13, at 234-37. *See also* ITA, *infra* note 76. The author recommends that India adopt the most progressive stance, the one taken by the Third Wave. *See infra* notes 112-14, 137-39.

57. 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).

signatures and do not grant a monopoly to any one of them. Examples of permissive jurisdictions include the majority of states in the United States, the United Kingdom,[58] Australia and New Zealand.[59]

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

C. The Third Wave: A Hybrid

Singapore was in the vanguard of the Third Wave. In 1998, this country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce.[60] 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 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.[61]

---

58. For concise coverage of the United Nations, European Union, British and American law of digital signatures, *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, 11-43 (2005).

59. Fischer, *supra* note 24, at 234-37.

60. *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), *available at* http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (last visited Oct. 25, 2006) [hereinafter MLEC].

61. Electronic Transactions Act, 1998 (Sing.), *available at* http://agcvldb4.agc.gov.sg/ (last visited Oct. 25, 2006). 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 that

Since 1998, a number of other countries have joined the Third Wave by emulating the hybrid perspective of Singapore. This moderate position has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European Union's E-Signatures Directive,[62] Japan,[63] Vanuatu,[64] Taiwan,[65] Lithuania,[66] Iran,[67] South Korea,[68] Barbados,[69] Hong Kong,[70] Bermuda,[71] Pakistan,[72] Dubai,[73] Azerbaijan[74] and most recently,

---

the other types of electronic signatures: (1) digital signatures are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carry a legal presumption of reliability and security – these presumptions are not given to other forms of electronic signatures; and (2) although all forms of electronic signatures are allowed to be used in Singapore, its electronic signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the authenticity and integrity of electronic messages affixed to electronic signatures. *Id.* *See* Stephen E. Blythe, *Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality*, 33 OHIO N. U. L. REV. (forthcoming 2006).

62. Council Directive 1999/93, *supra* note 8, at art. 2(1). *See* Stephen E. Blythe, *supra* note 58, at 19-20.

63. Stephen E. Blythe, *Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access*, J. INTERNET L. 20, 24 (1996).

64. Stephen E. Blythe, *South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga*, 10 J. S. PAC. L. (forthcoming 2006), *available at* http://www.paclii.org/journals/fJSPL/vol10/Blythe%20%20South%20Pacific%20Computer%20Law.shtml.

65. Stephen E. Blythe, *Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security*, Proceedings of the Sixth Annual Hawaii International Conference on Business (2006).

66. Stephen E. Blythe, *Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions*, 8 BARRY L. REV. (forthcoming 2006).

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

68. 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).

69. Stephen E. Blythe, *The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute*, 16 CARIBBEAN L. REV. (forthcoming 2006).

70. *See* Stephen E. 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 (2005).

71. Fischer, *supra* note 24, at 234-37.

72. Stephen E. Blythe, *Pakistan Goes Digital: The Electronic Transactions Ordinance as a Facilitator of Growth for E-Commerce*, J. ISLAMIC ST. PRAC. INT'L L., 2006, at 5.

73. Stephen E. Blythe, *The Dubai Electronic Transactions Statute: A prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries*, 22 J. ECON. & ADMIN. SCI. (forthcoming 2006).

74. Stephen E. Blythe, *The Azerbaijan E-Commerce Statutes: Contributing to*

China.[75]

IV. INDIA'S INFORMATION TECHNOLOGY ACT

India's Information Technology Act ("ITA")[76] was enacted on June 9, 2000.[77] The ITA's purposes are to: (1) recognize the legal validity of electronic transactions that are used in E-commerce; (2) promote the growth of E-government, i.e., the acceptance and utilization of documents in electronic form by government departments; and accordingly, (3) to amend the criminal law, evidence law and banking law insofar as they are affected by the legal recognition of electronic transactions.[78] Ostensibly, deference was shown by the drafters of the ITA to the United Nations' Model Law on Electronic Commerce.[79] The following items are excluded from coverage of the ITA: (1) negotiable instruments; (2) powers-of-attorney; (3) trusts; (4) wills and other testamentary dispositions; (5) contracts for the sale or transfer of real property; and (6) other documents or transactions which may be specified by the government in the *Official Gazette*.[80]

A. Legal Recognition of Electronic Form

1. Satisfaction of Writing Requirement

If a law mandates that information must be in writing, that requirement is deemed to have been satisfied if the information is contained in an electronic record, provided it can be retrieved and referenced at a later time.[81]

2. Satisfaction of Authentication Requirement

An electronic record is deemed authenticated if signed with a

---

Economic Growth and Globalization in the Caucasus Region, 12 COLUM. J. E. EUR. L. (forthcoming 2006).

75. Stephen E. Blythe, *China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce*, 6 CHI.-KENT J. INTELL. PROP. (forthcoming 2006).

76. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [hereinafter ITA].

77. *Id.* at pmbl.

78. *Id.*

79. *Id.* The author disagrees. India's ITA is more akin to the First Wave with its technological exclusivity than the hybrid perspective taken by the Third Wave which was championed in the U.N.'s Model Law on Electronic Commerce. *See infra* notes 111-114.

80. ITA, *supra* note 76, § 1(4).

81. *Id.* § 4.

digital signature.[82]

3. Satisfaction of Signing Requirement

If a law mandates that a document must have been signed in order to incur a legal right, that requirement is deemed to have been met if an electronic document is signed with a digital signature.[83]

4. Satisfaction of Government Filing, Issuance or Payment

If government departments prescribe it, the electronic form is allowed for: (1) filing of documents with the government; (2) the government's issuance of licenses or permits; and (3) payment of money to or by the government.[84] However, the government department in question may specify the form or method of filing, issuance or payment to be used.[85]

Notwithstanding the above, no government department is required to use the electronic form for filings, issuances or payments.[86]

5. Satisfaction of Retention Requirement

If a law mandates for a document to be kept in storage, that requirement may be met by the retention of an electronic document, provided: (1) the information is accessible and can be retrieved at a later time; (2) the document is stored in its original format or in a format that facilitates an accurate representation of the information contained in the original document; and (3) the electronically-stored document identifies the "origin, destination, date and time of [dispatch] or receipt."[87]

---

82. *Id.* § 3. The government reserves the right to issue rules relating to: (1) the specific characteristics of digital signature required to be used; (2) the "manner and format" of the attachment of the digital signature to the electronic document; (3) methods of identification of the subscriber; (4) security procedures and methods; and (5) other necessary matters. *Id.* § 10. Attachment of a digital signature, "with its grammatical variations and cognate (*sic*) expressions," to an electronic record, requires "adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature." *Id.* § 2(1)(d).

83. ITA, supra note 76, § 5.

84. *Id.* § 6(1).

85. *Id.* § 6(2).

86. *Id.* § 8. The author perceives this "voluntary" E-government to be a defect and will recommend that E-government change to a "compulsory" system. *See infra* notes 137-39.

87. ITA, *supra* note 76, § 7(1). Automatically-generated data relating to the dispatch or receipt of an electronic document do not have to be stored. *Id.* Furthermore, this provision is inapplicable if any other law expressly allows retention in electronic form. *Id.* § 7(2).

6. Satisfaction of Publication Requirement

If a law mandates that a public notice be made in the *Official Gazette*, that mandate shall be deemed to have been met if it is published in the *Electronic Gazette*.[88]

B. Electronic Transaction Rules

1. Attribution Rules

It may be assumed that an electronic record was sent by the Sender if: (1) the sender sent it; (2) the sender's agent sent it; or (3) the sender's computer information system, which the sender or her agent programmed, automatically sent it.[89]

2. Acknowledgement of Receipt

If the sender, who has requested acknowledgement of receipt, does not specify the form or method to be used by receiver, then the receiver may employ: (1) any type of communication, manual or automated; or (2) conduct sufficient to show the sender that the reception has occurred.[90]

If the sender has instructed the receiver that the electronic record will have no legal impact until the sender is in receipt of the acknowledgement, then the electronic record is assumed to not have been sent until the sender is in receipt of the acknowledgement from the receiver.[91] On the other hand, if the sender has not placed conditionality upon her receipt of the acknowledgement, and the sender has not received an acknowledgment within a reasonable time or within a previously-specified time, then the sender: (1) after informing the receiver that no acknowledgement has been received, give the sender a reasonable time deadline by which the acknowledgement must be received; and (2) if the sender is not in receipt of the acknowledgement by the deadline, then the sender may take the legal position as if the electronic record had never been sent and exercise her rights accordingly.[92]

---

88. *Id.* § 8. If the notice is actually published on more than one day, the official date of publication will be deemed to be the first day of publication. *Id.*

89. ITA, *supra* note 76, § 11.

90. *Id.* § 12(1).

91. *Id.* § 12(2).

92. *Id.* § 12(3).

C. Time and Place of Transmission and Reception[93]

1. Time of Dispatch

An electronic record will be assumed to have been sent when it enters a computer information system outside the control of the sender.[94]

2. Time of Reception: Receiver Has Designated Location

If the receiver has indicated a specific computer information system for the electronic record to be sent to: (1) the assumed time of reception is when it enters the designated computer information system; or (2) if it enters another computer information system of the receiver that is not the designated one, then the assumed time of reception is when the receiver retrieves the electronic record from the computer information system.[95]

3. Time of Reception: Receiver Has Not Designated Location

If the receiver has not designated a specific computer information system for the electronic record to be sent to, then the assumed time of reception is when the electronic record enters any computer information system of the receiver.[96]

4. Place of Transmission and Reception

The electronic record is assumed to have been sent from the sender's place of business, and the electronic record is assumed to have been received at the receiver's place of business.[97] If either the sender or the receiver has more than one place of business, the place will be assumed to be the principal place of business.[98] If either the sender or the receiver does not have a place of business, then the assumed location will be the sender or receiver's "usual place of residence."[99]

---

93. The rules in this section may be modified by agreement of the parties. *Id.* § 13.

94. ITA, *supra* note 76, § 13(1).

95. *Id.* § 13(2)(a). This rule applies even if the location of the computer information system differs from the deemed place of reception pursuant to ITA § 13(3). *Id.* § 13(4).

96. *Id.* § 13(2)(b). This rule applies even if the location of the computer information system differs from the deemed place of reception pursuant to ITA § 13(3). *Id.* § 13(4).

97. ITA, *supra* note 76, § 13(3).

98. *Id.* § 13(5)(a).

99. *Id.* § 13(5)(b). In the case of a corporation, the "usual place of residence" will be the jurisdiction in which it is registered or incorporated. *Id.* § 13(5)(c).

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

In the eyes of the ITA, electronic records and digital signatures do not have an equal degree of security. Some of them are more secure than others. "Secure" electronic records and digital signatures have more security than non-secure ones.

To be considered a "secure" electronic record, a security procedure must have been applied to it. It will carry the secure status from the time of first application until the time of verification.[100]

To be considered a "secure" digital signature, a security procedure accepted by all parties must confirm that at the time of attachment (to an electronic record), the digital signature was: (1) unique to the subscriber; (2) identified the subscriber; and (3) was under the sole control of the subscriber and was connected to the electronic record so that if any changes were made to the electronic record, the digital signature would automatically be invalidated.[101]

The government is mandated to prescribe the security procedures to be used in reference to the two preceding paragraphs. Of course, the specific security procedures expected to be employed will change over time as new technological developments occur. However, the following general considerations will be taken into account in setting the requirements: (1) type and characteristics of the transaction; (2) technological knowledge and expertise of the parties; (3) other parties' experience in similar transactions; (4) whether other security options have been offered to other parties, but rejected by them; (5) the cost of other security procedures; and (6) the security procedures most commonly used in similar transactions or communications.[102]

D. Regulation of Certification Authorities

1. Controller of Certifying Authorities

The government has appointed an officer to hold the post of Controller of Certifying Authorities (hereinafter "Controller").[103] The Controller, along with Deputy Controllers and Assistant Controllers appointed by the Controller,[104] bear the general responsibility to the

100. *Id.* § 14.

101. ITA, *supra* note 76, § 15.

102. *Id.* § 16.

103. *Id.* § 17(1).

104. *Id.* § 17(3). The Controller is authorized to delegate in writing any of his powers to the Deputy Controllers and Assistant Controllers. *Id.* § 27. The Controller's powers are the same as those granted to Income-tax authorities pursuant to Chapter XIII of the Income-

government[105] for regulation of Certification Authorities ("CA")[106] and for investigation of any alleged violations of the ITA.[107]

With respect to CAs, the Controller will have the following specific responsibilities:

1. licensing of CAs;[108]

2. supervising CAs and controlling how they conduct their business;[109]

3. developing and disseminating standards to be applied by CAs in the verification of digital signatures;[110]

4. certifying CAs' public keys;[111]

5. regulating CAs' computer information systems and facilitating their establishment;[112]

6. informing CAs as to the form to be used in the certificates they issue, and the required information to be included in the certificates, including the subscribers' public keys;[113]

7. regulating the relationship between CAs and their subscribers;[114]

8. maintaining an up-to-date database of information pertaining to CAs and the certificates they have issued;[115] and

9. determining the terms and conditions of appointment of auditors to

---

tax Act of 1961, and are subject to the limitations stated in that Act. ITA, *supra* note 76, § 28(2).

105. *Id.* § 17(2).

106. *Id.* § 18.

107. *Id.* § 28(1). Pursuant to this investigatory power, the Controller has the right to obtain access to a CA's computer equipment and records if he has reasonable cause to believe the CA has violated the ITA. Furthermore, the CA and its employees are bound to assist the Controller to obtain access to the materials needed to conduct the investigation. *Id.* § 29.

108. ITA, *supra* note 76, § 18(d).

109. *Id.* §§ 18(a), (e), (f), (h), (m).

110. *Id.* § 18(c).

111. *Id.* § 18(b).

112. *Id.* § 18(j). CAs are mandated to have a computer information system with secure hardware and software, and acceptable security procedures. Their services must be reliable and the privacy of digital signatures must be maintained. ITA, *supra* note 76, § 30.

113. *Id.* § 18(g).

114. *Id.* §§ 18(k), (l).

115. *Id.* § 18(n). The database is ordinarily available for public viewing at the Controller's website.

periodically audit CAs and their activities.[116]

E. *Licensing of Certification Authorities*

No person or entity may act as a CA unless it holds a license issued by the Controller.[117] This is known as a "compulsory"[118] CA system because holding a license is a requirement.[119]

1. *General Application Requirements*

No one should apply for a CA's license unless she expects to be able to show she possesses the requisite: (1) knowledge, abilities and skills; (2) number of personnel;[120] (3) capitalization; and (4) physical assets, including computer equipment and suitable worksite.[121]

2. *The Documents Required to be Submitted in the Application*

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

1. an application document in the form prescribed by the government;[122]

2. the application fee to be prescribed by the government, which will not exceed 25,000 rupees;[123]

3. the applicant's Certification Practice Statement ("CPS");[124]

---

116. ITA, *supra* note 76, § 18(i).

117. *Id.* § 21.

118. China is another example of a nation with a compulsory CA system.

119. Some other jurisdictions, e.g. Hong Kong and Korea, have a voluntary CA system. In them, it is possible to have CAs in business which are unlicensed. However, even in voluntary jurisdictions, it is difficult to find unlicensed CAs because there are two important disadvantages in being unlicensed: (1) the government will ordinarily increase the level of potential legal liability to those entities; and (2) any electronic documents or electronic signatures they have verified will not be accorded full-fledged legal status, which would severely reduce the likelihood they could survive. Hence, even in a "voluntary" jurisdiction, the practicalities of the situation almost compel the entity to get a license. *See* Blythe, *supra* note 70; Blythe, *supra* note 68.

120. Furthermore, a CA is responsible for informing its employees of the requirements imposed by the ITA and its implementation regulations, rules and orders. ITA, *supra* note 76, § 31.

121. *Id.* § 21.

122. *Id.* § 22(1).

123. *Id.* § 22(2)(c). Twenty-five thousand rupees is approximately U.S. $ 553. Currency and Foreign Exchange, http://www.xe.com (last visited Oct. 24, 2006).

124. ITA, *supra* note 76, § 22(2)(a). The idea of a CPS originated in the United States. The prospective CA, or licensed CA, must draft the CPS. The CPS will contain the detailed

4. a statement regarding the types of identification documents the applicant will present;[125] and

5. other documents specified by the government.[126]

3. License Renewal

An application for renewal must be filed with the Controller at least 45 days before the expiration date of the license.[127] The application must be made on the form prescribed by the Controller and the renewal fee (not to exceed 5,000 rupees) must be paid.[128]

4. Controller's Decision and Due Process for Applicant

Within a reasonable time after receipt of an application for a license or for its renewal, the Controller should make a decision. If the Controller decides to reject an application for a license or for its renewal, the applicant should be afforded a "reasonable opportunity" to make a pertinent statement in rebuttal.[129]

5. License Suspension and Revocation

The Controller is authorized to suspend a CA's license (for a period not to exceed ten days) if there is reasonable cause to believe that the CA has:

1. made a false statement or submitted false documents in the application, e.g., misrepresentation of financial or physical resources;

2. did not comply with its own CPS or other conditions which were the basis upon which the license was granted;

3. violated the standards required in ITA § 20(2)(b); or

4. failed to abide by the ITA or pertinent regulations, rules or orders.[130]

Before the expiration of the ten-day suspension period, the CA

---

policies, procedures and rules which the CA expects to implement in the execution of its duties and responsibilities. Indian Law defines a CPS as "a statement issued by a [CA] to specify the practices that the [CA] employs in issuing Digital Signature Certificates." *Id.* § 2(1)(h). *See* Information Security Committee, *supra* note 35.

125. ITA, *supra* note 76, § 22(2)(b).

126. *Id.* § 22(2)(d).

127. *Id.* § 23.

128. *Id.* § 23(b).

129. *Id.* § 24.

130. ITA, *supra* note 76, § 25.

should be given a reasonable opportunity to make a statement in rebuttal.[131] After the CA has been given its due process, the Controller must make a decision to: (1) extinguish the suspension and reinstate the validity of the CA's license; (2) extend the suspension period beyond the initial ten-day period; or (3) revoke the CA's license.[132] Any CA whose license has been suspended or revoked is forbidden to issue certificates[133] and must immediately surrender its license to the Controller.[134]

If suspension or revocation occurs, the Controller is required to give written notice to the CA and to keep an electronic copy of said notice in its database. If two or more databases are maintained, the notice should be filed in all of them. The databases should be accessible 24 hours a day, seven days a week. Additionally, if considered necessary by the Controller, the notice may be published in "other media."[135]

F. Duties of a Certification Authority

1. Public Disclosures

If a CA's application for a license is granted, the license will be issued to the new CA and must be displayed in a "conspicuous place" at the CA's worksite.[136]

A licensed CA is also mandated to publicly disclose: (1) the public key which has an interactive relationship with the CA's private key (the CA's private key is the one used to sign its subscribers' Certificates); (2) whether its Certificate containing that public key has been suspended or revoked; (3) its CPS; and (4) other facts which may have a detrimental impact upon the reliability of the Certificates that it issues or its ability to conduct certification services.[137] Furthermore, a CA has a duty to disclose to all affected parties any fact or situation which may have a detrimental impact upon: (1) the integrity of its computer information system; or (2) the reliability of its outstanding

131. *Id.* § 25.

132. *Id.* § 25(2).

133. *Id.* § 25(3).

134. *Id.* § 33(1). It is a criminal offense for a CA to refuse to surrender a license after it has been suspended or revoked. The maximum punishment is six months imprisonment, a fine of 10,000 rupees, or both. ITA, *supra* note 76, § 33(2).

135. *Id.* § 26.

136. *Id.* § 32.

137. *Id.* § 34(1).

Certificates.[138] A CA must follow the designated procedures stated in its CPS for dealing with that fact or situation.[139]

G. Issuance and Management of Certificates

1. Application for Certificate

A person desiring to have a Certificate issued to verify his digital signature should apply to a CA using the prescribed form.[140] The CA will inform the applicant of the fee,[141] requisite documents pertinent to proof of identification, and significant information contained in its CPS or a copy of the CPS.[142] Within a reasonable time after receipt of the application, the CA must make a decision as to whether to accept or reject the application. If the decision is negative, the applicant shall be informed of the reasons in writing and afforded due process by granting an opportunity to contest the decision. In order for the decision to be positive, the CA must be satisfied that: (1) the subscriber holds the private key corresponding to the public key that is listed in the Certificate; (2) the private key is capable of generation of a digital signature; and (3) the public key can be used to verify the digital signature executed by the private key.[143]

2. A Certificate's Legal Significance

A third party doing business with a subscriber may find himself in receipt of an electronic document that has been signed with the subscriber's digital signature. In that situation, he needs a confirmation that the electronic document was actually signed by the purported signatory and that the document has not been altered since it was signed. These needs serve to highlight the legal significance of the CA's representations in the Certificate: (1) that the CA has met all of the mandates of the ITA and its implementation regulations, rules and orders; (2) that the subscriber has accepted the Certificate and it has been published and is accessible to relying third parties; (3) that the subscriber holds the private key which has an interactive relationship

138. *Id.* § 34(2).

139. ITA, *supra* note 76, § 34(2).

140. *Id.* § 35(1).

141. *Id.* § 35(2). The fee may not exceed 25,000 rupees, which is approximately U.S. $553. *See* Currency and Foreign Exchange, *supra* note 123. However, different fees may be charged different classes of applicants. ITA, *supra* note 76, § 35(2).

142. ITA, *supra* note 76, § 35(3).

143. *Id.* § 35(4).

with the public key, and they comprise a "functioning key pair;" (4) that all information contained in the Certificate is accurate; and (5) that the CA is not aware of any significant information which would have a detrimental impact upon the aforementioned representations.[144]

3. Suspension of a Certificate

A CA may suspend a Certificate based on the following grounds: (1) when the subscriber or his agent so requests; or (2) when this action would serve the "public interest."[145]

The CA must inform the subscriber of the suspension as soon as possible.[146] The suspension status must be published at all of the CA's public information repositories and at all of its websites.[147] The suspension period is limited to 15 days unless due process has been given to the subscriber by affording him an opportunity to contest the suspension.[148]

4. Revocation of a Certificate

The Controller may revoke a Certificate on the following grounds: (1) when the subscriber or her agent so requests; (2) when the subscriber is deceased; (3) if the subscriber is an entity (not an individual), when the subscriber has become insolvent and has entered into bankruptcy proceedings; (4) when any requirement mandated for issuance of the Certificate has not been complied with; (5) when the subscriber supplied a false material fact which has been placed in the certificate; or (6) when the CA's computer system or the private key is no longer secure, and this has materially detrimental effect upon the reliability of the Certificate.[149]

No revocation is allowed unless due process has been given to the subscriber by affording him an opportunity to contest the revocation.[150] If the Certificate is revoked, that status must be published at all of the CA's public information repositories and at all of its websites,[151] and the CA must promptly inform the subscriber of the revocation.[152]

---

144. *Id.* § 36.
145. *Id.* § 37(1)(a-b).
146. *Id.* § 37.
147. ITA, *supra* note 76, § 39.
148. *Id.* § 37(2).
149. *Id.* § 38(1)-(2).
150. *Id.* § 38(3).
151. *Id.* § 39.
152. ITA, *supra* note 76, § 38(4).

H. Duties of a Subscriber

1. Generation of Keys

If the subscriber has agreed to solely generate the public key and the private key, then the subscriber must do so using the agreed-to security procedure. The public key (corresponding to the private key, which will be retained by the subscriber) will be listed in the Certificate.[153]

2. Acceptance of the Certificate

The subscriber is considered to have legally accepted a Certificate from the CA when he or his agent: (1) presents it to one or more persons; (2) places it in a repository; or (3) leads other parties to believe that he ratifies and agrees with the information contained in the Certificate.[154] To all persons who "reasonably rely" on the Certificate's information, the subscriber, by his acceptance, warrants that: (1) the subscriber holds the private key which corresponds to the public key which is included in the Certificate and is entitled to hold it; (2) all statements made by the subscriber to the CA in the application process are true, and all documentary evidence presented to the CA in the application process are valid; and (3) to the best of the subscriber's knowledge, all information contained in the Certificate is true.[155]

3. Maintenance of Security of the Private Key

A subscriber has a duty to exercise reasonable care in the maintenance of security over the private key which corresponds to the public key contained in the Certificate. The subscriber should do everything reasonably possible to ensure that the private key is not lost, stolen, or ends up in the possession of an unauthorized person.[156]

If the private key has been lost or stolen, or if its security has been compromised in any manner, the subscriber should inform the CA at once. The subscriber remains liable for damages caused by the insecurity of the private key until the CA has been notified.[157]

---

153. *Id.* § 40.
154. *Id.* § 41(1).
155. *Id.* § 41(2).
156. *Id.* § 42(1).
157. ITA, *supra* note 76, § 42.

I. Network Service Providers

Network service providers ("NSP") are intermediaries[158] which provide internet or telecommunications services. As a general rule, NSP are not subject to any civil or criminal penalties merely because they have enabled subscribers to gain access to information or data of a third party. However, the NSP will be subject to potential liability if it had knowledge that any facts or statements were being disseminated by the third party in violation of the ITA, its implementation regulations, or pertinent orders.[159]

J. Civil Offenses

1. Damage of a Computer Information System

It is a civil wrong to knowingly, and without necessity: (1) obtain access to a computer without permission, or deny access to persons authorized to obtain access; (2) destroy, alter, or incapacitate any part of a computer information system; (3) download or copy material from a computer; (4) introduce a virus or other contaminant into a computer information system; (5) disrupt the operations of a computer; and (6) use a computer without paying for its use. It is also a civil wrong to coerce, influence, assist, or entice another person into the commission of these wrongful acts.[160] A wrongdoer will be liable to damaged parties in an amount not to exceed 10 million rupees.[161]

2. Failure to Cooperate with Controller

It is also a civil wrong for a CA to refuse to cooperate with the Controller in the exercise of its oversight function. A CA must provide requested documents or reports to the Controller in a timely manner. Failure to do so may result in a fine not to exceed one lakh and 50,000 rupees for each refusal. Furthermore, a CA is obligated to file returns, information and books to the Controller from time to time. If the CA fails to do so, it may be fined up to 5,000 rupees for each day it is late.[162]

---

158. Indian law defines an intermediary as "any person who on behalf of another person receives, stores or transmits [an electronic] message or provides any service with respect to that message." *Id.* § 2(w).

159. *Id.* § 79.

160. *Id.* § 43.

161. *Id.* § 43. Ten million rupees is approximately $216,843. Currency and Foreign Exchange, *supra* note 123.

162. ITA, *supra* note 76, § 44. Five thousand rupees is approximately. $109. Currency

3. Default Penalty

If the ITA or its implementation regulations are violated, but no civil penalty is specified, the residuary punishment will be: (1) maximum liability of 25,000 rupees payable to the person incurring damages as a result of the wrongful acts; or (2) a maximum fine of 25,000 rupees if a CA fails to cooperate with the Controller.[163]

K. Computer Crimes

India claims "long arm" jurisdiction over foreign parties committing criminal acts outside of India which have an effect on a computer information system located within India.[164] A court may order law enforcement authorities to seize computer equipment that is suspected of having been used in the commission of a computer crime.[165] It is possible for more than one punishment to be administered for commission of the same unlawful acts if more than one criminal law has been violated.[166]

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[167] used for a computer, computer program, computer system, or computer network, when the computer source code is legally required to be retained for a specific duration. The punishment for this crime is imprisonment (three years' maximum),

---

and Foreign Exchange, *supra* note 123.

163. ITA, *supra* note 76, § 45. Furthermore, the Controller may compound any of the contraventions which are listed in ITA Chapter X. For example, if a wrongdoer commits a second or third offense of the same infraction during a three-year-period, the punishment meted out may be greater for the second offense, and still greater on the third offense. However, if the second offense occurs three or more years after the occurrence of the first offense, the "slate is wiped clean" and the punishment assigned is for a first offense of that infraction. *Id.* § 63. Still further, any penalty that remains unpaid will be treated as an "arrear of land revenue" and the CA's license, or the Certificate, will be suspended until the penalty has been paid. *Id.* § 64.

164. *Id.* § 75.

165. *Id.* § 76. Alternatively, if information relevant to a computer crime is believed to be contained within computer equipment in possession of a person who is not suspected of commission of a crime, then the court may undertake other action "as it may think fit." ITA, *supra* note 76, § 76.

166. *Id.* § 77.

167. *Id.* § 65. Computer source code is defined as "the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form." *Id.*

or a fine (200,000 rupees' maximum), or both.[168]

2. Hacking into a Computer

It is a crime to gain access to a computer information system without authorization from its owner or rightful custodian, with knowledge that such action is likely to destroy, delete, or modify information contained therein, or reduce its value. The punishment will be a fine (200,000 rupees maximum), or imprisonment (three years maximum), or both.[169]

If the hacking occurs in a computer information system that has been designated by a government department as a "protected system," the maximum punishment will be 10 years of imprisonment, plus a fine.[170]

3. Electronic Publication of Obscene Materials

It is a crime to publish obscene materials in electronic form on either the internet or in telecommunications media. The punishment for the first occurrence will be a fine (100,000 rupees maximum), imprisonment (five years maximum), or both. Those committing subsequent offenses of the same type will be punished with imprisonment of 10 years, a fine (200,000 rupees maximum), or both.[171]

4. Failure to Maintain Confidentiality of Private Information

It is a crime for a person to disseminate private information to an unauthorized person, notwithstanding the fact that the information was accessed and obtained with authorization. This includes information from records, books, registers, correspondence, documents, or other materials. Depending upon the seriousness of the dissemination, the punishment will be imprisonment (two years maximum), a fine (100,000 rupees maximum), or both.[172]

5. Provision of False Information

It is a crime for an applicant for a Certificate to provide false

168. Id. § 65. Two hundred thousand rupees is approximately $4378. Currency and Foreign Exchange, *supra* note 123.

169. ITA, *supra* note 76, § 66. Two hundred thousand rupees is approximately $4378. Currency and Foreign Exchange, *supra* note 123.

170. ITA, *supra* note 76, § 70.

171. *Id.* § 67.

172. *Id.* § 72. One hundred thousand rupees is approximately $2189. Currency and Foreign Exchange, *supra* note 123.

information to a CA or to the Controller. The punishment will be imprisonment (two years maximum), a fine (100,000 rupees maximum), or both.[173]

6. CA's Failure to Follow Controller's Orders

If the Controller believes a CA (or its employees) is in contravention of the ITA or its implementation regulations, the Controller may order the CA to perform certain acts, or to cease the performance of certain acts. If the CA fails to adhere to the Controller's orders, the CA may receive a maximum punishment of three years of imprisonment, a maximum fine of 200,000 rupees, or both.[174]

7. Subscriber's Failure to Assist in National Security Matter

If the national security is at stake, the Controller is authorized to order any government agency to "intercept any information transmitted through any computer resource." It is a crime for a subscriber or any person in control of a computer resource to refuse to offer the resource or assistance in decryption of the information sought by the government. Maximum punishment is seven years of imprisonment.[175]

8. Non-Fraudulent Use of Invalid Certificate

It is crime to publish a Certificate in the following situations: (1) the CA listed in the Certificate did not issue it; (2) the subscriber listed in the Certificate has not accepted it; or (3) the Certificate was suspended or revoked (unless such publication was done to confirm a digital signature executed *prior* to the suspension or revocation). The maximum punishment is a jail term of two years, a fine of 100,000 rupees, or both.[176]

9. Fraudulent Use of Invalid Certificate

It is a crime for a person with a fraudulent purpose to create, publish or make available a bogus Certificate, pretending to the world that it is a good Certificate, when in fact it is invalid. The maximum punishment will be two years of imprisonment, a fine of 100,000

173. ITA, *supra* note 76, § 71. One hundred thousand rupees is approximately $2189. Currency and Foreign Exchange, *supra* note 123.

174. ITA, *supra* note 76, § 68. Two hundred thousand rupees is approximately $4378. Currency and Foreign Exchange, *supra* note 123.

175. ITA, *supra* note 76, § 69.

176. *Id.* § 73. One hundred thousand rupees is approximately $2189. Currency and Foreign Exchange, *supra* note 123.

rupees, or both.[177]

10. Offenses By Business Firms

If the offender is a business firm, every person who "was in charge" of the company at the time of the wrongful acts is individually liable. However, it is possible for an individual manager to avoid liability if he can prove that he was unaware of the wrongful acts or that he did his best to prevent their occurrence. But note: if the manager did not learn of the wrongful acts due to the fact that he was neglectful, that is insufficient to escape liability; an "ostrich defense" is not allowed![178]

L. Adjudication of Violations of the ITA

1. Adjudicating Officers Appointed by Controller

The Controller appoints adjudicating officers to hear and resolve alleged violations of the aforementioned rules and determines the geographical locations where each may exercise jurisdiction. After giving all parties an opportunity to present their cases at a hearing, the officer will render a decision in the matter.[179] The officer will take into account: the wrongdoer's "gain of unfair advantage;" the amount of loss caused by the wrongful acts; and the number of times the wrongdoer committed the acts.[180] Penalties will be imposed or awards will be made on a case-by-case basis. The qualifications for adjudicating officers will be stated by the government and will include both information technology experience and legal/judicial experience. The officers' authority will be both civil and criminal in nature.[181]

2. Cyber Regulations Appellate Tribunal

The government of India is authorized to establish one or more Cyber Regulations Appellate Tribunals, and to specify the "matters and places" pertinent to their jurisdiction.[182] Their general purpose is to serve as the first appellate level to which cases may be appealed from decisions of the Control Board or adjudicating officers established in

177. ITA, *supra* note 76, § 74. One hundred thousand rupees is approximately $2189. Currency and Foreign Exchange, *supra* note 123.

178. *Id.* § 85(2).

179. *Id.* § 46(2).

180. *Id.* § 47.

181. *See id.* § 46.

182. ITA, *supra* note 76, § 48.

the ITA.[183] If the parties previously agreed to an order of an adjudicating officer, it may not be appealed.[184] An appeal to the Tribunal must be filed within 45 days from the date on which the aggrieved party received a copy of the order of the Controller or the adjudicating officer.[185] The Tribunal will make every effort to dispose of each appeal within six months from the date it is received.[186] The Tribunal will hear all parties to the controversy and may affirm the previous order, modify it or set it aside.[187] All parties and the concerned Controller or adjudicating officer will be given a copy of the Tribunal's order.[188]

3. The Presiding Officer of the Cyber Appellate Tribunal

The Tribunal shall consist of one Presiding Officer appointed by the government.[189] The Presiding Officer must be: (1) a High Court Judge; (2) a former High Court Judge; (3) qualified to be a High Court Judge; or (4) a present or former member of the Indian Legal Service and either currently holds, or has held, a Grade I post in that Service for a minimum of three years.[190] The term of office of the Presiding Officer ends at the end of five years of service or when he becomes 65 years of age, whichever occurs first.[191] The Presiding Officer's salary, benefits and terms and conditions of service will be determined by the government, but the salary and benefits may not be reduced during the Officer's tenure, and neither may the terms and conditions of employment become more disadvantageous during his tenure.[192] The Presiding Officer is entitled to have a suitable staff to assist him.[193]

---

183. *Id.* § 57(1). No other court has jurisdiction to meddle in the affairs of an adjudicating officer under the ITA or in the affairs of the Appellate Tribunal by issuing an injunction against their orders or acts, so long as the adjudicating officer or the Tribunal has been properly empowered by the ITA. *Id.* § 61.

184. *Id.* § 57(2).

185. *Id.* § 57(3). However, for good cause shown, the Tribunal may allow an appeal to be filed beyond the 45 day cutoff. ITA, *supra* note 76, § 57(3). The Limitation Act of 1963 applies to the Tribunal. *Id.* § 60.

186. *Id.* § 57(6).

187. *Id.* § 57(4).

188. *Id.* § 57(5).

189. ITA, *supra* note 76, § 49. In order to challenge a decision of an Appellate Tribunal, it is an insufficient ground to question the validity of the governmental order of appointment of the Presiding Officer. Furthermore, it is also an insufficient ground to point to an alleged defect in the constitution of an Appellate Tribunal. *Id.* § 55.

190. *Id.* § 50.

191. *Id.* § 51.

192. *Id.* § 52.

193. ITA, *supra* note 76, § 56(1).

If a vacancy occurs in a Presiding Officer's position (other than a temporary leave of absence), the government will appoint a new person to fill the vacancy and the proceedings will continue under the new Officer.[194] If the Presiding Officer decides to resign his position, he must submit a handwritten letter of resignation to the government; the Officer is ordinarily expected to continue in office for three months following submission of the letter, until a successor has been appointed or his term expires, whichever occurs first.[195] The Presiding Officer may be impeached and removed from his office if it is proven through a legal proceeding before a Judge of the Supreme Court that the Officer has committed misbehavior or lacks capacity; in that proceeding, the Presiding Officer must be afforded his right of due process by being informed of the charges and having a reasonable opportunity to be heard.[196]

4. Procedure and Powers of the Cyber Appellate Tribunal

The procedures to be employed by the Cyber Appellate Tribunal are not those specified in the Code of Civil Procedure of 1908. Instead, the Cyber Appellate Tribunal will use the procedures according to the principles of natural justice. So long as the Appellate Tribunal adheres to the ITA, the Appellate Tribunal is empowered to establish its own procedures including the venue at which it holds its sessions.[197]

In order for the Appellate Tribunal to fulfill its functions in reference to a lawsuit, it is empowered similarly to other courts pursuant to the Code of Civil Procedure of 1908. Specifically, the Appellate Tribunal is empowered to: (1) compel attendance of witnesses; (2) examine witnesses under oath; (3) compel production of paper and electronic documents; (4) admit evidence in the form of an affidavit; (5) order that witnesses or documents be examined by the issuance of a commission; (6) reconsider its own decisions; (7) issue a default judgment for failure to appear or, in the alternative, make a decision *ex pane*; or (8) deal with other matters as prescribed.[198]

A person appearing before the Appellate Tribunal may either present his case in person or may have his case presented by an

194. *Id.* § 53.

195. *Id.* § 54(1).

196. *Id.* § 54(2). The government may establish procedural rules pertaining to the investigation of the alleged misbehavior or incapacity of the Presiding Officer. *Id.* § 54(3).

197. ITA, *supra* note 76, § 58(1).

198. *Id.* § 58(2).

attorney.[199] The Appellate Tribunal is *quasi*-civil and *quasi*-criminal in nature.[200]

5. Appeal to High Court

Decisions rendered by the Appellate Tribunal may be appealed to the High Court. The appeal must ordinarily be filed at the High Court within 60 days after the decision has been received. However, for good cause shown, the High Court may allow up to an additional 60 days in which to file the appeal.[201]

M. Implementation Rules and Regulations

Rules and regulations are necessary to implement the ITA. In development of rules and regulations, the government and the Controller are given advice and suggestions by the Cyber Regulations Advisory Committee.[202]

1. Governmental Rules

The federal government is generally authorized to make rules relating to the implementation of the ITA. Without limiting the coverage of this general mandate, the government is empowered to make rules pertinent to the following: (1) means of authentication using digital signatures; (2) the electronic forms and types of digital signatures required to be used in filings of E-documents and E-payments with the government, and in governmental transmissions of E-documents and E-payments to citizens;[203] (3) the security procedure to be employed in reference to a "secure" E-record and "secure" digital signature; (4) qualifications required to be met by the Controller and his assistants; (5) security standards expected to be used by the Controller; (6) qualifications required to be met by an applicant for a CA's license, the application form to be used, the amount of application fee, and documents required to be submitted with the application; (7) the period

199. *Id.* § 59.

200. *Id.* § 58. Proceedings before the Appellate Tribunal are deemed to be a judicial proceeding pursuant to sections 193, 196 and 228 of the Indian Penal Code. Further, pursuant to section 195 and Chapter XXVI of the Code of Criminal Procedure, the Cyber Appellate Tribunal will be considered a civil court. *Id.*

201. ITA, *supra* note 76, § 62.

202. *Id.* § 88.

203. The state governments are also authorized to enact rules pertinent to the implementation of the E-government aspects of the ITA. Specifically, state governments should enact rules relating to their receipt and transmission of electronic documents, and the receipt and transmission of electronic payments. *Id.* § 90.

of validity of a CA's license; (8) form to be used in application for renewal of CA's license, and amount charged to renew the license; (9) application form to be used in application for Certificate and the fee to be charged; (10) adjudication officers' experience, qualifications and procedure to be followed at their hearings; and (11) the Cyber Appellate Tribunal: remuneration of Presiding Officer and his staff, procedure for investigation of Presiding Officer's alleged misconduct, forms to be used in appealing to this forum and fees, and civil court powers.[204]

Notification of proposed rules must be made in the *Official Gazette* and the *Electronic Gazette*.[205] Furthermore, before they become effective, the rules will be presented to both houses of Parliament for their comments, suggestions and modifications.[206]

2. Controller's Regulations

The Controller reserves the general right to issue implementation orders and directives applicable to all concerned parties.[207] Furthermore, the Controller is specifically authorized to issue regulations governing: (1) the CA's maintenance of a database of information pertinent to its outstanding Certificates; and (2) the legal recognition of foreign CAs; (3) the issuance of licenses to CAs; (4) operating and security standards applicable to CAs; (5) reporting requirements of CAs; (6) statements and materials mandated to be submitted with the application for a Certificate; and (7) the method of communication used by a subscriber to inform a CA that a private key's security has been compromised.[208] Before the regulations become effective, they will be sent to both houses of Parliament for their review and possible amendment.[209]

N. Amendments of other Prior Acts

Several other statutes were amended by the ITA to bring them up-to-date with the nuances of a digital world. They are: (1) the Indian Penal Code;[210] (2) the Indian Evidence Act;[211] (3) the Bankers' Books

204. *Id.* § 87(2).
205. *Id.* § 87(1).
206. ITA, *supra* note 76, § 87(3).
207. *Id.* § 89(1).
208. *Id.* § 89(2).
209. *Id.* § 89(3).
210. *Id.* § 91. The amendments are contained in ITA, First Schedule.
211. ITA, *supra* note 76, § 92. The amendments are contained in ITA, Second Schedule.

Evidence Act;[212] and (4) the Reserve Bank of India Act.[213]

V. SUMMARY AND RECOMMENDATIONS

A. Summary: India's Information Technology Act

The ITA was enacted by the government of India in 2000. The purposes of the ITA are to recognize the legal validity of electronic contracts of E-commerce, to promote E-government and to amend several statutes in need of updating to accommodate the electronic form. Documents pertinent to the following must be in paper form and are therefore excluded from coverage of the ITA: wills, trusts, sale or transfer of real property, negotiable instruments, powers-of-attorney and other transactions specified by the government.

The ITA provides that electronic documents and digital signatures are legally valid. Electronic documents may be used to satisfy a statutory writing requirement, authentication requirement, retention requirement, publication requirement, and governmental filing, issuance, or payment requirement. A digital signature may be used to comply with a statutory requirement for a signatory to affix a handwritten signature on paper. The ITA distinguishes "secure" electronic documents and digital signatures from ordinary ones. To comply with the requirements for secure status, the electronic document or digital signature must utilize more stringent security procedures.

The ITA includes detailed rules governing the negotiation and consummation of an electronic contact. Attribution rules pertain to whether there is a legal presumption that an electronic message was actually sent by the party who purportedly sent it. Rules regarding acknowledgement of receipt concern the means of acknowledgement by the receiver to the sender; they are also concerned with the legal effect of a sender informing the receiver that his message will have no legal impact until the sender receives an acknowledgement. There are also rules relating the legally presumed place of transmission and reception of an electronic message, and the legally presumed time at which an electronic message was transmitted and received.

Detailed rules are provided for the regulation of Certification Authorities (CA), third parties whose duty is to vouch for the authenticity and integrity of an electronic message that has been signed with a digital signature. The ITA establishes the office of Controller of

212. *Id.* note 76, § 93. The amendments are contained in ITA, Third Schedule.

213. *Id.* § 94. The amendments are contained in ITA, Fourth Schedule.

CAs to implement the regulatory rules. India has adopted a compulsory system of CA licensing; no party may offer certification services without a license. A prospective CA must apply to the Controller for a license and submit supporting evidence of expertise, personnel, capitalization, physical assets, and a suitable worksite. The Controller must rule on the application within a reasonable time. If the decision is negative, the applicant will be granted an opportunity to contest the decision.

A CA's license is renewable. A CA's license may be suspended or revoked for good cause shown. A CA is mandated to: publicly display its license; issue certificates to successful applicants; and manage outstanding certificates by keeping the information in them up-to-date and suspending or revoking them for good cause shown.

Subscribers whose signatures are confirmed by certificates also have responsibilities: generate the public key and private key if they agree to do so; give full and truthful answers to all questions posed by the CA; ensure that the public key contained in the certificate corresponds to the private key he holds; ensure that the information in the certificate is accurate, and promptly inform the CA if he learns otherwise; maintain security of the private key; and promptly inform the CA if the security is compromised.

Network service providers, including firms providing internet or telecommunications services, have limited liability as a result of enabling subscribers to gain access to information or data of a third party. However, they may be liable if they have knowledge of the dissemination of facts or statements by a third party in violation of the ITA.

Under the ITA, it is a civil offense for any person or entity to knowingly damage a computer information system, or for a CA to fail to cooperate with the Controller in the exercise of its regulatory function. Under the ITA, it is a crime for a person or entity to: tamper with computer source documents; hack into a computer; electronically publish obscene materials; fail to maintain confidentiality of private information gleaned from a computer information system (even if the person was authorized to obtain the information); give false information to the Controller or to a CA; fail to obey an order given by the Controller to a CA; fail to obey an order given by the Controller to a subscriber in reference to a national security matter; or misuse a certificate in either a non-fraudulent or a fraudulent manner. If the violator is an entity, its managers at the time of the wrongful acts may be individually liable, unless they can show that they were unaware of the acts or took steps to prevent them.

The Controller appoints adjudicating officers to hear both civil and criminal cases relating to the ITA and to render decisions accordingly. The decisions of the adjudicating officers may be appealed to the Cyber Regulations Appellate Tribunal, consisting of one Presiding Officer who is empowered to establish his own procedures and venue so long as the ITA is not violated. Decisions rendered by the Appellate Tribunal may be appealed to the High Court.

The federal government of India and the Controller are empowered to issue regulations necessary to implement the ITA and will be given advice in this regard by the Cyber Regulations Advisory Committee.

B. Recommendations for Improvement of India's ITA

India's Information Technology Act establishes a good basic framework for the attainment of secure E-commerce transactions. However, the following amendments are recommended for its improvement.

1. Join the Third Wave

The ITA does not define "electronic signature." The only type of electronic signature that is defined is the digital signature. This and other evidence leads the author to conclude that the ITA is a member of the First Wave of electronic signature laws. In order to explicitly join the most progressive generation of electronic signature laws—the Third Wave—the ITA needs to adopt a very inclusive definition of "electronic signature" and to emphasize that all types of electronic signatures are accepted. Commensurate with Third Wave status, the ITA should also continue to grant most-favored status to the digital signature and to maintain a comprehensive system of regulation of Certification Authorities.

2. Eliminate the Exclusion for Wills

The ETL excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature affixed to it in order to be enforceable. This exclusion should be eliminated.[214]

214. There is evidence that the aversion to electronic wills is beginning to dissipate. In 2005, Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature. *See* Chad Michael Ross, Comment, *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).

3. Add More Consumer Protections for Participants in E-commerce

India needs to enact a general consumer protection statute applicable to all internet consumers. The Republic of Tunisia can be used as a model for good consumer protections. The Tunisian E-commerce statute gives consumers: (1) a "last chance" to review an order before it is entered into; (2) a 10 day window of opportunity to withdraw from an agreement after it has been made; (3) a right to a refund if the goods are late or if they do not conform to specifications; and (4) no risk during the 10-day trial period after goods have been received. Tunisian E-consumers enjoy some of the best protections in the world.[215]

4. Replace the Controller's Adjudicating Officers with Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology ("IT") Courts should be established as a court-of-first-instance for them. They should replace the adjudication officers which are appointed by the Controller. The IT Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an IT expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the IT person would be required to hold a graduate degree in an IT-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business

---

215. Electronic Exchanges and Electronic Commercial Bill, arts. 24-35 (Tunis), *available at* http://www.bakernet.com/ecommerce/Tunisian%20National%20Certification%20Agency.pdf (last visited Nov. 7, 2006). *See* Stephen E. Blythe, *Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures*, 20 ARAB L. Q. 240 (2006). One of the few nations that may offer better consumer protections is Korea. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act. *See* KOREAN LEGISLATION RESEARCH INSTITUTE, *Act on the Consumer Protection in the Electronic Commerce Transactions*, 13 STATUTES OF THE REPUBLIC OF SOUTH KOREA 481-485 [hereinafter CPA]. The CPA was originally enacted by law No. 6687, March 30, 2002 and amended by acts 7315 and 7344 of December 31, 2004 and January 27, 2005, respectively. The CPA recently underwent a major overhaul with substantial amendments in act 7487 of March 31, 2005; those amendments became effective on April 1, 2006. For coverage of the CPA, *see* Blythe, *supra* note 68. Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-commerce transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Blythe, *supra* note 67.

administration and have managerial experience. The E-commerce law of the Kingdom of Nepal can be used as a model.[216]

5. Make E-Government Mandatory

Presently, the ITA allows governmental departments to interact with citizens via acceptance or issuance of electronic documents. The governmental departments of India are not required to convert to the electronic form, however. This should be changed. Whenever feasible, mandatory (not merely permissive) requirements for governmental agencies to accept and issue electronic documents should be implemented. This would expand E-government, resulting in more convenience for citizens, greater efficiency, and less cost. The E-Government Act of Finland can be used as a model.[217]

216. Electronic Transactions Ordinance No. 32 of the Year 2061 B.S. (2005), § 60-71 (Nepal), *available at* http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf (last visited Nov. 7, 2006).

217. Act on Electronic Services and Communications in the Public Sector (Fin), *available at* http://www.finlex.fi/en/laki/kaannokset/2003/en20030013.pdf (last visited Nov. 7, 2006).