CYBERLAW: A COMPARATIVE STUDY OF THE LEGAL FRAMEWORK FOR E-COMMERCE IN INDIA AND THE UNITED STATES

VIVEK MALIK*
MARY VIRGINIA MOORE**

I. INTRODUCTION

Technological advancements in the field of communications have greatly shortened the distance across the globe. Revolutionary changes in both synchronous and asynchronous communication have taken place as a result of the popularity of the Internet. Vast amounts of information, formerly expensive and difficult to obtain, now proliferate on the Internet. The approach to business transactions has changed, as new technology replaces traditional modes of doing business. Consequently, regulations to monitor activities over the Internet must be implemented in order to keep pace with the new advances in information technology.

Among the world's technologically developed nations, India was the twelfth country to develop cyber law regulations, following such pioneers as the United States, Singapore, France, Malaysia and Japan.[1] India's Information Technology Act of 2000 (ITA) draws its inspiration from the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and the United Nations General Assembly on January 30, 1997.[2]

The ITA focuses on two different facets of the technological revolution. First, it seeks to provide legal recognition of electronic transactions by acknowledging the use of electronic communication as an alternative to paper-based communication and information storage. Second, the ITA aims to regulate and control cyber crimes and other related offenses.[3]

The ITA was approved by the Union Cabinet on May 13, 2000 and was passed in both houses of the Parliament on May 17, 2000.[4] It received presidential assent on June

---

*MBA Candidate, Southeast Missouri State University
**Associate Professor of Business Law, Southeast Missouri State University

[1] Interview by Rajitha Saleem with Pavan Duggal, Founder & President, Cyberlaws.net, *DQ Week*, *available at* http://www.ciol.com(last visited Feb. 13, 2002).

[2] C.I.S. No. 21 of 2000, Information Technology Act, 2000 of the Ministry of Information Technology, New Delhi, Oct. 17, 2000 (Preamble citing UN resolution A/RES/51/162), *available at* http//:www.indialawinfo.com/bareacts/ift.htm (last visited Sept. 16, 2001) [hereinafter ITA]. Note to reader: some of the spelling of terms in the ITA has been changed in this paper to reflect United States usage.

[3] *Id.*

[4] Ashit Shah, *The Information Technology Act, 2000: A legal Framework for E-Governance* , *available at* http://www.sudhirlaw.com/cyberlaw-itact.htm (last visited Oct. 31, 2001).

19, 2000[5] and was implemented as the "Information Technology Act, 2000" after the Central Government issued a formal notification in the Official Gazette on October 17, 2000.[6]

The ITA contains 13 chapters,[7] 93 sections and 4 schedules. For consistency, each of the four schedules of the ITA amends provisions of existing statutes.[8] Two significant aspects of the ITA include:

1. Communications-contractual framework: legal recognition and the evidentiary value of electronic records, authentication, rules governing digital signatures, and rules governing appointment and regulation of certification authorities (CAs).[9]
2. Cyber Adjudication: civil and criminal violations, penalties, and the establishment of the Cyber Regulatory Appellate Tribunal (CRAT) & the adjudicating authority.[10]

It is interesting to note that the ITA was one of the first pieces of legislation in India to be open for public comment prior to its finalization. The public's favorable response indicates support for what the public believes is necessary legislation.

In the United States, legislation has been introduced at both the federal and state levels affecting the governance of e-commerce. The National Conference of Commissioners on Uniform State Laws (NCCUSL) is now engaged in drafting

---

[5] ITA, *supra* note 2, also *available at* http//: www.laws4india.com/cyberlaws/itamendment1.asp(last visited Dec. 13, 2001).

[6] Gazette of India, Part II, § 3(i)(Oct. 17, 2000), *available at* http//:www.mit.gov.in/rules/actnotification.htm.

[7] *See* ITA, *supra* note 2.

Chapter I (Sections 1-2) describe the scope and applicability of the act and provides definitions.

Chapter II (section 3) deals with the digital signatures, their authentication and related details, such as asymmetric cryptosystems.

Chapter III (sections 4-10) establishes the legal status of electronic records and digital signatures and describes their use by the Central Government. Section 9 places limitations on compelling total electronic governance.

Chapter IV (sections 11-13) discusses the contractual aspects of the electronic records such as attribution, acknowledgement, time and place of dispatch and receipt of electronic records.

Chapter V (sections 14-16) deals with the security issues concerning electronic records and digital signatures.

Chapters VI, VII & VIII (sections 17-42) provide a legal regulatory framework for the appointment of Certifying Authorities (CAs) and their powers, as well as the issuance of digital signatures. The contractual rights and duties of certifying authorities vis-à-vis a subscriber are also prescribed. In addition, the central government's powers to make rules and regulations relating to the business operations aspect of the CAs, including the recognition of foreign CAs, are described.

Chapters IX, X & XI (sections 43-78) deal with infringements, cyber offenses and penalties. These chapters also describe the establishment of the office of Adjudicating Officer and the Cyber Regulations Appellate Tribunal (CRAT).

Chapter XII (section 79) consists of a single section detailing the liabilities of network service providers.

Chapter XIII (section 80-93) contains miscellaneous provisions, such as police powers, the overriding effect of the Act, and powers of the central and state governments to create legislation. The last four sections contain amendments to various statutes.

[8] *See* INDIAN PEN. CODE (1860) , Indian Evidence Act (1872), Bankers' Books Evidence Act (1891); and Reserve Bank of India Act (1934).

[9] ITA, *supra* note 2, chs. IV, V, VI.

[10] *Id.* at chs. IX, X and XI.

legislation to deal with e-commerce and Internet issues. To that end, the NCCUSL has proposed two acts: the Uniform Computer Information Transactions Act (UCITA)[11] and the Uniform Electronic Transaction Act (UETA).[12] The NCCUSL has also drafted major revisions to the Uniform Commercial Code (UCC) to govern e-commerce. The key issues associated with e-commerce contracts that are addressed in these statutes include uniformity between electronic and paper records, attribution procedures, and electronic signatures.[13] The UETA is primarily a procedural statute that deals broadly with e-commerce and contract law, while the UCITA and Article 2 of the UCC as amended are both substantive statutes that interject missing terms into incomplete contracts. Revisions in Article 2, section 2B of the UCC apply to the sale of goods regardless of whether or not the sale involves e-commerce.[14]

This paper is a comparative study of the legal framework for e-commerce in India and the United States. The paper begins by summarizing, explaining and evaluating important provisions in the Information Technology Act of 2000. In sections two and three, the paper compares the ITA with similar laws in the United States in two contexts: the communications-contractual framework and electronic governance. The paper points out similarities and differences in each country regarding the status of electronic records, attribution of electronic records and its procedures, authentication issues, evidentiary issues and other legal issues. Section four discusses the function of electronic business in both countries. Cyber flouting is discussed in section five and recent developments are shared in section six. Concluding remarks are presented in section eight.

II. COMMUNICATIONS-CONTRACTUAL FRAMEWORK

Given the global nature of the Internet, entering into a contract and doing business online is not as secure as the traditional method of contracting. The most pressing concern regarding e-commerce contracts is the legal recognition of electronic records. With the enactment of ITA, India legally recognized electronic records in instances where the law requires a writing.[15] In the United States, similar provisions in the UETA,[16] UCITA and the revised Article 2B of the UCC create parity between electronic records and paper records.[17]

A second challenging issue for e-business is the security of the online contracts. One way to make these contracts secure is by legally recognizing electronic signatures as legitimate mechanisms for authenticating non-face to face electronic transactions. There are various forms of electronic signatures, such as asymmetrical cryptography (digital signatures), biometric devices (identifies individuals by their physical characteristics) and symmetrical cryptography (use of personal identifications, such as pin codes and

---

[11] DAVID BRAUMER & J.C. POINDEXTER, CYBERLAW AND E-COMMERCE 58 (2000). Virginia and Maryland are the only two states that have adopted the UCITA to date.
[12] *Id.* at 65. To date, forty states have adopted the UETA.
[13] *Id.* at 56.
[14] *Id.* at 62.
[15] ITA, *supra* note 2, at ch. III, § 4 .
[16] UNIF. ELECTRONIC TRANSACTIONS ACT § 7 cmt. 1 (1999). "The medium in which a record, signature, or contract is created, presented or retained does not affect it's legal significance."
[17] BAUMER & POINDEXTER, *supra* note 11, at 65. *See also, infra*, Appendix A.

passwords).[18] The most reliable and popular form of electronic signatures is the digital signature based on the Public Key Infrastructure (PKI). There are significant differences between other types of signatures and digital signatures, including application process results and reliability for legal purposes.[19]

A branch of applied mathematics called cryptographics is used to create and verify digital signatures. The process involves two parts: creation of the digital signatures by the signator of the document; and verification of the signatures by the receiver of the digital document. A more fundamental process called the hash function is used for both the creation and verification of digital signatures. The hash function creates a code much smaller than the message to create an effect in the digital framework. The software then transforms the hash result into a digital signature by reference to the signator's private key, which makes the signature unique to both the message and the private key used to create it.[20]

In India, the ITA has adopted the Public Key Infrastructure, which uses hash functions[21] and asymmetric cryptosystems[22] as a means of securing electronic transactions. A subscriber[23] uses the digital signature for authentication of an electronic record. This system works on a two-way principle: "a private key is used to create a digital signature whereas a public key is used to verify the digital signatures."[24] Both the private key and the public key are distinctive for each subscriber and together they create a functioning key pair. Under the ITA, a digital signature would be deemed "secure" provided the following condition is met. After application of security procedures, the signature must prove to be (a) unique to the subscriber; (b) able to identify the subscriber affixing it; (c) created and used under the exclusive control of the subscriber; and (d) annulled upon the tampering of the electronic record.[25] If the transaction is between private parties, those interested parties must agree on the security procedures to be applied. If the transaction is commercial, the Central Government dictates the applicable securities procedures.[26]

Certifying Authorities (CAs) appointed under the ITA are empowered to authenticate these digital signatures. These CAs are licensed to issue Digital Signature Certificates (DSCs).[27] The DSCs offered are organized in various classes depending upon the security levels, price, period of validity and restrictions on the use of the DSC. Foreign CAs are recognized, subject to regulations and prior approval of the Central Government. Prior to the commencement of any cross-certification operations between an Indian CA and a foreign CA, the government Controller must specifically approve the arrangement.[28]

---

[18] Renaud Sorieul, *The UNCITRAL's Model Law on Electronic Signatures* (2001), *available at* http://droit-internet-2001.univ-paris.fr/pdf/ve/sorieul_ve.pdf (last visited Jan. 27, 2002).

[19] D.P. MITTAL, LAW OF INFORMATION TECHNOLOGY (CYBER LAW) 61-62 (2000).

[20] Robin Whittle, *Public Key Authentication Framework: Tutorial*, *at* http//: www.ozemail.com.au/~firstpr/crypto/pkaftute.htm (last modified June 2, 1996).

[21] ITA, *supra* note 2, at ch. II, § 3.

[22] *Id.* at ch. I, § 2(1)(f).

[23] *Id.* at ch. I, § 2(1)(zg). The digital signature certificate is issued to the subscriber.

[24] Shah, *supra* note 4, at 2.

[25] ITA, *supra* note 2, at ch. V, § 15.

[26] *Id.* at ch. III, § 6.

[27] *Id.* at ch. VI, § 21.

[28] *Id.* at ch. VI, § 19. *See also* Rule 12 (2), The Information Technology (Certifying Authorities) Rules (2000)(India).

In the United States,[29] electronic records authentication and attribution issues have been addressed at both the state and federal levels. The first state legislation to this effect was the Utah Digital Signatures Act of 1995.[30] Some states have adopted comprehensive regulatory guidelines, while others have brief directives that simply authorize the use of electronic or digital signature technology.[31] At the federal level, the issue has been addressed by the UETA,[32] UCITA[33] and UCC.[34] "The UCC is even more liberal in accepting as a signature, 'any symbol executed or adopted by a party with present intention to authenticate a writing.'"[35]

The Electronic Signature in Global and National Commerce Act (the E-sign Act)[36] is another significant federal law in the United States. Electronic signature laws are designed to help remove barriers to conducting business online and to enable and promote trust and predictability among the parties engaged in online business.[37] These laws facilitate online business transactions by using digital signatures, ensuring validity and enforceability of electronic contracts and providing legal protection for the contracting parties. The definition of digital signatures is not restricted to only those created by using cryptography. Rather, the scope of the definition is extended by allowing different techniques to effectuate authentication, such as using simple passwords, digital thumbprints, retinal scanning devices and third party services for the creation and verification of digital signatures using cryptography.

In the United States, laws adopting a technologically neutral approach to the authentication of electronic signatures are more flexible with regard to the legal recognition of electronic signatures.[38] Despite this, most government agencies and other organizations seek to use a PKI framework to safeguard their data and securely link their networks to the Internet.[39] Illinois is currently the only state that is cooperating with the federal government in terms of using the PKI encryption framework.[40]

E-signature laws in United States provide room for innovation by recognizing signatures created abroad.[41] This truly reflects the theme of UNCITRAL's Model Law on

---

[29] *See infra* Appendix A.
[30] Thomas J. Smedinghoff & Ruth Hill Bro, *Electronic Signature Legislation*, *at* http://www.findlaw.com (last visited Jan. 20, 2002).
[31] Lawrence Cohen, *E-commerce Law Click on the Dotted Line 'E-Signatures' come of age and make the future of E-commerce a little brighter* N.J. L.J (Aug. 20, 2001), *available in* LEXIS-NEXIS Academic Universe.
[32] BAUMER & POINDEXTER, *supra* note 11, at 56.
[33] *Id.*
[34] *Id.*
[35] *Id.* at 77 ((quoting UCC § 102(6)).
[36] Cohen, *supra* note 31, at 1.
[37] Smedinghoff & Bro, *supra* note 30, at 2.
[38] John D. Gregory, *Canadian and American Legislation on Electronic Signatures with Reflection on the European Union Directives*, *available at* http//:droit-internet-2001.univ-paris1.fr/pdf/ve/Gregory_j.pdf (last visited Jan. 27, 2002).
[39] Dan Balaban, *Fortifying the Network*, 2 CARD TECH. 70 (May 2001), *available in* LEXIS-NEXIS Academic Universe.
[40] Institute of Management Administration (IOMA), *How PKI Technology Solves e-signature Security Problems*, MANAGING HR INFORMATION SYSTEMS, (Nov. 2001), *available in* LEXIS-NEXIS Academic Universe.
[41] Gregory, *supra* note 38.

Electronic Signatures, which is to combine flexibility and legal security to preserve technological neutrality.[42]

Admissibility of the electronic records in a court of law is the next area of concern. Important evidentiary issues in all legal proceedings involving e-commerce include authenticity, reliability and admissibility of the electronic records produced. To address these issues, the ITA has amended the language in The Indian Evidence Act of 1872 to include secured electronic records and digital signatures.[43] Now, the Indian Evidence Act incorporates provisions for electronic contracts, secure electronic documents, electronic messages and electronic records.[44] Other statutes have also been expanded to support electronic evidence.[45]

In the same context, the UETA, which is a procedural statute, provides for the admissibility of electronic records or signatures and prevents omitting evidence merely because of its electronic form.[46]

III. ELECTRONIC GOVERNANCE

Besides regulating E-commerce, the ITA seeks to promote internal electronic communication and transactions within India's governmental structure. Chapter III of the ITA deals with the use of electronic records within the Central Government and its agencies. The Central Government uses electronic records to expedite many common tasks, such as:[47]

1. granting licenses and permits, and issuing approvals or sanctions;
2. publishing rules, notices or regulations in the electronic Gazette;
3. enabling citizens to file applications or government forms electronically; or
4. enabling citizens to make payments and retain records electronically.

Even though the ITA provides the statutory framework for electronic transactions, the Central Government is not compelled to use an electronic medium to preserve official records or transact official business. The use of electronic records and digital signatures

---

[42] Sorieul, *supra* note 18, at 3.

[43] THE SECOND SCHEDULE: AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872, C.I.S. No. 21 of 2000, Information Technology Act, 2000 of the Ministry of Information Technology, New Delhi, Oct. 17, 2000 *available at* http//:www.indialawinfo.com/bareacts/ift.htm (last visited Sept. 16, 2001). *See infr*a Appendix A.

[44] *Id.* at §§ 85A, 85B and 88A.

[45] THE FIRST SCHEDULE: AMENDMENT TO THE INDIAN PENAL CODE, 1860, C.I.S. No. 21 of 2000, Information Technology Act, 2000 of the Ministry of Information Technology, New Delhi, Oct. 17, 2000, *available at* http//:www.indialawinfo.com/bareacts/ift.htm (last visited Sept. 16, 2001);
THE THIRD SCHEDULE: AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT, 1891, C.I.S. No. 21 of 2000, Information Technology Act, 2000 of the Ministry of Information Technology, New Delhi, October 17, 2000, *available at* http//:www.indialawinfo.com/bareacts/ift.htm (last visited Sept. 16, 2001);
THE FOURTH SCHEDULE: AMENDMENTS TO THE RESERVE BANK OF INDIA ACT OF 1934, C.I.S. No. 21 of 2000, Information Technology Act, 2000 of the Ministry of Information Technology, New Delhi, Oct. 17, 2000 *available at* http//:www.indialawinfo.com/bareacts/ift.htm (last visited Sept. 16, 2001).

[46] UNIF. ELECTRONIC TRANSACTIONS ACT § 13 (1999) [hereinafter UETA]

[47] ITA, s*upra* note 2, § 6.

is at the Central Government's discretion and the power to govern both lies squarely with the Central Government by virtue of the ITA.[48]

Similarly, in the United States the UETA provides optional provisions for governmental agencies to create and retain records in electronic form and also to convert written records to electronic records.[49] Electronic records may be used to satisfy existing statutes, regulations or rules that require written records, such as contracts or checks,[50] but at the same time, there is restrictive use of E-signatures for sensitive documents, such as "wills, notice of cancellation of health insurance benefits and product safety recalls."[51]

IV. ELECTRONIC BUSINESS

Many businesses have benefited from the use of faster and cheaper communication methods. Readily available access to various services through the Internet, such as online ordering, online payment, broadcasting, and search and recovery, has encouraged businesses to conduct commerce transactions electronically. Rather than using paper-based agreements, e-mail is sometimes used to create contracts and to exchange commitments. As applied to contract transactions, the ITA is intended to be read in conjunction with existing laws, including the Indian Contract Act. According to the Indian Contract Act, the formation of any contract involves three main components: (1) an offer;[52] (2) an acceptance to the unaltered offer;[53] and (3) some contractual consideration.[54] However, determining the moment of contract formation online may not be very clear.

Traditional contract law has been challenged on several fronts by the anonymous nature of the Internet. For example, the identity of the parties, the time of dispatch or receipt of the offer or acceptance, and the place of communication are not easily recognizable when the transaction takes place in cyberspace. Other important related issues addressed in the Information Technology Act include: (1) attribution of electronic records;[55] (2) acknowledgement of receipt;[56] (3) time and place of dispatch and receipt of electronic records;[57] and (4) international transactions.

According to Chapter IV of the ITA, "An electronic record shall be attributed to the originator a) if it was sent by the originator himself; b) by a person who has the authority to act on behalf of the originator with respect to that electronic record; or c) by an information system programmed by or on behalf of the originator to operate automatically."[58] This section uses the principle of agency to attribute the electronic

---

[48] *Id*. at § 9.
[49] UETA §§ 17, 18, & 19 (1999).
[50] *Main provisions of electronic signatures act*, CONSUMER FIN. SERVICES L. REP., Mar. 19, 2001, at 1, *available in* LEXIS-NEXIS Academic Universe.
[51] Jube Shiver, Jr., *House Signs Off on Bill Validating Online Contracts*, LOS ANGELES TIMES, June 15, 2000, at 1, *available in* LEXIS-NEXIS Academic Universe.
[52] INDIAN CONTRACT ACT § 3 (1872).
[53] *Id.* § 7.
[54] *Id.* § 8.
[55] ITA, *supra* note 2, at ch. IV, § 11. *See also infra* Appendix A.
[56] *Id.* at ch. IV § 12.
[57] *Id.* at ch. IV § 13.
[58] *Id.* at ch. IV § 11. *See also infra* Appendix A.

record to the originator when a person (under the originator's authority) other than the originator has performed that action.

Absent an agreement by the addressee and the originator or a stipulation by the originator as to a particular method of acknowledging receipt of the electronic communication, the ITA describes a default acknowledgement process whereby "an acknowledgement may be given by: a) any communication by the addressee, automated or otherwise; or b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received."[59]

To determine when an offer or acceptance becomes effective, the time and place of communication must be considered. An electronic record is dispatched from the principal place of business of the originator the moment it enters a system under the control of someone other than the originator. Communication is received at the principal place of business of the addressee the moment it enters the computer resource under the control of the addressee.[60]

Additional complications arise when international business is transacted over the Internet. Generally, the laws of a party's own nation govern each party's entrance into a contract. Moreover, the laws of the country where the obligations are to be performed govern certain aspects of the transaction. The parties to the contract should agree as to which law will govern the contract. Absent such an agreement, the law of the nation having the most substantial connection to the transaction will be applied.[61]

In United States the laws relating to the formation of a contract have been revised to facilitate online contract formation. The "UICTA and revised Article 2 of the UCC allow intent to be *inferred* from the operations of electronic agents, and signatures (called authentication) can occur with a response to an invitation to click or accept."[62] Revisions to Article 2 of the UCC permit *additional terms* to be included in the definition of acceptance, even if they materially alter the contract.[63]

V. CYBER ADJUDICATION

Cyber crime is an emerging issue that corresponds with the improvement and expansion of the Internet. Apart from the individual lawsuits, public interest litigation (PIL) is an important and viable legal method in India of ensuring justice and protecting the general public against cyber crime. Since the enactment of the ITA, several PIL lawsuits have been filed addressing issues, such as online child pornography and Internet fraud. With increased awareness among the masses about online crimes and offenses, a significant rise is expected in the number of lawsuits. These PILs will serve as a powerful tool to curb online cyber crimes. In India, the National Association of Software and Service Companies (NASSCOM) is working in association with the Ministry of Information Technology to fight such cyber crimes.[64]

---

[59] *Id.* at ch. IV § 12.
[60] *Id.* at ch. IV § 13.
[61] ITA, *supra* note 2.
[62] BAUMER & POINDEXTER, *supra* note 11, at 67.
[63] *Id.* at 71.
[64] Aparna Achar, C*oncerns about India's new IT Bill*, BUS. & MGMT. PRACTICES, Aug. 2000, at 15, *available at* LEXIS-NEXIS Academic Universe.

A significant portion of the Indian Information Act of 2000 is dedicated to adjudication, liability, and defining the powers of the Cyber Regulations Appellate Tribunal (CRAT). The ITA attempts to establish distinct mechanisms for handling both civil and criminal infringements. If a criminal offense is suspected, a police officer is granted the power to investigate, to conduct searches and to make arrests under the Code of Criminal Procedure (1973).[65] In civil cases, the adjudicating officer, who is appointed by the Central Government, is empowered to pass judgments and impose penalties.[66] The ITA also deals with the appointment of adjudicating officers, their qualifications and powers. The Act provides for appellate review of initial decisions made by the adjudicating officer.[67] Any further appeals are brought before the High Court.[68]

Chapter X of the ITA details the establishment of CRAT, its composition, qualifications of the presiding officer, terms and conditions of service (including salary and allowances), and procedures and powers of the tribunal.[69] Chapter XI outlines the powers of investigating officers, identifies various kinds of criminal offenses subject to fines, and provides for mandatory penalties, including imprisonment.[70]

Regardless of the place where the wrongdoing occurred and without respect to the nationality of the defendants, the ITA has an extraterritorial reach outside India with respect to any offense or breach committed, as long as the contravention involves a computer, computer system or network located in India.[71] Considering the complexity and multinational nature of Internet crimes and the different jurisdictions involved, enforcement of such extraterritorial powers will depend upon international cooperation.

VI. RECENT FINANCIAL DEVELOPMENTS

To take advantage of the fast, economical method of securities trading offered over the Internet, the Securities Exchange Board of India (SEBI) issued guidelines on January 31, 2000 for Internet-based securities trading and services. For legal purposes, the Information Technology Act, 2000 is applicable to all electronic contracts and transactions entered into under the SEBI guidelines.[72]

Advancements in technology have helped the banking industry to grow all over the world. Since the Reserve Bank of India issued Internet banking guidelines on June 14, 2001, India has legally recognized Internet banking. With an increase in awareness among the masses and with the development of an infrastructure to support Internet banking, a shift from traditional modes of banking to Internet banking is predicted in the near future. The free flow of money both from within the country and outside the country should help the Indian economy.

---

[65] ITA, *supra* note 2, at ch. XIII, § 80.
[66] *Id*. at ch. IX, § 46(5) .
[67] *Id*. at ch. X, § 57.
[68] *Id*. at ch. X, § 62.
[69] *Id*. at ch. X.
[70] *Id*. at ch XI.
[71] *Id*. at ch. XI, § 75.
[72] Securities and Exchange Board of India, *Internet Based Trading and Services*, SMDRP/POLICY/CIR-06/2000 (Jan. 31, 2000,) *available at* http://www.sebi.gov.in/circulars/2000/CIR062000.htm (last visited Feb. 14, 2002).

VII. CRITICISM OF ITA

Despite its expansive scope, the ITA omits several important issues. First, the provisions of the ITA are not applicable to provisions contained under Negotiable Instruments Act of 1881, Power-of-Attorney Act of 1882, and Indian Trust Act of 1882. Neither is the ITA applicable to a will or testamentary disposition as defined under Indian Succession Act 1925, nor to any contract for the sale of any interest in immovable property.[73] Second, the ITA only recognizes the PKI framework for authentication[74] and does not recognize any other form of authentication procedure. Third, search and arrest powers conferred on police officers are specific to public places, while no guidelines are provided for such powers in other locations. Since cyber crime more often than not occurs in the privacy of one's home or office, more specific regulations are needed to address this issue.[75] Fourth, no provisions in the ITA deal with protecting intellectual property rights or copyright violations over the Internet. Finally, no mention is made of taxation issues relative to the Internet.[76]

VIII. CONCLUSION

The ITA is India's initial legislation that provides a foundation for governing the growing information technology sector in India. The ITA provides a skeletal framework for Internet based transactions. More awareness among the masses and concerted efforts among governmental, non-governmental and other organizations to address issues of concern will help the legislature develop more focused legislation in the future.

Laws in United States govern significant aspects of the Internet, but still there is a need for a universal code that is applicable to everyone, everywhere. Different versions of cyber law regulations in different states may actually weaken the trust and consistency that the various state legislatures are trying to establish. Moreover, the United States should take the lead in developing a global framework for Internet operations in harmony with the nations of the world to provide a common platform for e-commerce.

---

[73] ITA, *supra* note 2, at ch. I, § 4 .
[74] Shah, *supra* note 4, at 2.
[75] Achar, *supra* note 64, at 15.
[76] Shah, *supra* note 4, at 8.

Appendix A

Comparison of The Legal Framework For E-Commerce between India and U.S.

INDIAN LAW	U.S. LAW
Information Technology Act, 2000.	1. Uniform Commercial Code (UCC) 2. Uniform Computer Information Transactions Act (UCITA) 3. Uniform Electronic Transaction Act (UETA)

Status of Electronic Records

Chapter III § 4	UCC § 2-210 (a) & UETA § 7
Guarantees legal validity of Electronic Records.	Establishes parity between paper records and electronic records.

Attribution of Electronic Records

Chapter IV §§ 11, 12 & 13	UCC § 2-211, UETA § 9 & UCITA § 213
Similarity Electronic Record is attributed to the originator if it is: 1. sent by the originator. 2. sent by person having authority on behalf of the originator. 3. sent by an automated/programmed system set up by the originator. *Difference* No details on procedures applied for attribution.	*Similarity* The electronic event is attributed to a person if it was the act of that person or his/her electronic agent. *Difference* The attribution procedure must be in compliance with established law and in the absence of such procedures, reliance can be made on commercially reasonable attribution procedures, such as the assent of both parties to the procedure.

Authentication Issues (Electronic Signatures)

Chapter II § 3	UCC § 2-210(a), UETA § 7 (d)
Similarity Recognizes digital signatures based on Public Key Infrastructure (PKI) framework. *Difference* Rigid - only accepts asymmetric mode of authentication (digital signatures based on PKI only)	*Similarity* Recognizes PKI framework for authentication of electronic records. *Difference* Flexible - recognizes other forms of electronic signatures based on biometric devices, or symmetrical cryptography, such as pin codes and passwords.

Evidentiary Issues

Schedule II	UETA § 13
Necessary amendments have been made to the Indian Evidence Act 1872 to make electronic records admissible as evidence in a court of law.	Recognizes electronic records for the purpose of admissibility as evidence in a court of law.

Other Issues

Digital Intellectual Property Issues	Digital Intellectual Property Issues
The ITA does not discuss digital IP issues, such as online copyright violation matters **Separate Courts** The ITA provides for the establishment of separate courts to hear matters exclusively related to cyber issues.	The UCITA devotes a fair amount of attention to the copyright issues and includes computer software, multimedia interactive products, computer data and databases, internet and other online information. **Separate Courts** There is no such provision for the creation of separate courts.