Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

E-Commerce & Law

Trends & Challenges

[S.Sai Sushanth]

***Abstract*— In the technology era, the traditional way of transacting business is replaced by electronic commerce popularly known as E-commerce. E-Commerce means using of information technology, computers and other electronic means to transact business by and between individuals and entities.**

E-commerce is one of the significant developments in the International Trade. It has provided many advantages besides many challenges.

The Information Technology Act 2000 is one of the primary laws which has promoted e-commerce, e-governance and has provided legal recognition to e-records and e-transactions.

Cyber law in India tires to attend these challenges and requires compliance of IT Laws by business houses engaging in e-commerce. The Indian Information Technology Act, 2000 make it mandatory to set up corporate compliance programs including cyber law compliance program.

Keywords*— *E-Commerce, Cyber law, IT Act, Mobile Commerce, Social Commerce, Data protection.

I. Introduction

Rise in information technology has revolutionarized the world into a cyber world. The communication, business, interactions, transactions are using cyber platform today. Commerce is also using electronic means to conduct its commercial activities by way of Electronic Commerce.

Electronic Commerce also referred to as E-Commerce can be explained as buying and selling products through electronic means. It includes internet, computers, computer networks, computer resources.

II. E-Commerce & IT Act

E-Commerce is the buying and selling products using World Wide Web, internet. E-business means conducting commercial activities via computers and relative technologies such as Internet.

E-commerce forms a part of e-business, specifically trading aspect (e-business). E-governance is government making all its operations using electronic medium. E- Commerce is a part of E-governance.

S.Sai Sushanth
Cyber Laws Knowledge Centre
India

Information Technology Act also known as IT Act is considered as Indian Cyber Law. The IT Act came into force in the year 2000. The fundamental objective of IT Act is

- To promote e-governance of which an essential part is e-commerce
- To provide legal recognition to electronic records and transactions carried out by way of electronic data interchange.

III. Types of E-Commerce

The following are different types of e-commerce

1) Business to Commerce (B2C)

The basic concept of this model is to sell the product online to the consumers.

2) Business to Business (B2B)

This model defines that Buyer and Seller are two different entities. It is similar to manufacturer issuing goods to the retailer or wholesaler.

3) Consumer to Consumer (C2C)

There is no major parties needed but the parties will not fulfill the transactions without the program which is supplied by the online market dealer such as eBay.

4) Peer to Peer (P2P)

Assists people to instantly share related computer files and computer sources without having to interact with central web server.

IV. E-Commerce & Law

There are various legal aspects surrounding E-Commerce. Some of them are explained as:-

A. E-Contracts

A valid and legally binding contract is the heart of e-commerce. (Online contracts)

IT Act 2000 – deals with Contractual aspects of use of Electronic Records such as

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

- Acknowledgement – Sec 12(1) of IT Act
- Time and Place of Dispatch and Receipt- Sec 13 of IT Act

Internet communication does not consist of a direct line of communication between the sender and receiver of e-mail as in ordinary means of communication. [1]

The message is broken into chunks in the process of delivery. This raises issues of the exact time of communication of acceptance of the contract as such a time is critical for determination of the rights of the parties.

E- Contracts are also called as Cyber Contracts, Online Contracts.

E -Contract: Contract entered through the medium of internet and software, World Wide Web, Exchange of e-mail stating offers, Acceptance of terms and condition of a particular transaction, Software installation.

E-contracts are conceptually very similar to traditional (paper based) commercial contracts, because of the ways in which it differs from traditional commerce; electronic commerce raises some new and interesting technical and legal challenges.

B. Online Identity

Transactions on the Internet, particularly consumer-related transactions, often occur between parties who have no pre-existing relationship, which may raise concerns of the person's identity with respect to issues of the person's capacity, authority and legitimacy to enter the contract. Digital signatures, is one of the methods used to determine the identity of the person.

C. Digital Signature

The digital signature is not infallible it is only computationally infeasible. The rise in the information technology is leading to further developments. The IT ACT 2000 also was amended in 2008, instead of digital signatures, a technology neutral term - electronic signature was added.

The regulatory framework with respect to digital signatures is governed by the provisions of the IT Act. However, various countries have different legislations regulating digital signatures.

D. Security

Internet Security is of immense importance to promote e-commerce. Companies that keep sensitive information on their websites must ensure that they have adequate security measures to safeguard their websites from any un-authorized intrusion. A company could face security threats externally as well as internally.

Apart from adequate security measures, appropriate legal documentation would also be needed. For example, a company could have an adequate security policy that would bind all the people working in and with the company. A company could also be held liable for inadequate security procedures on its website.

For example- a person decided to sue Nike because the Nike's website was hacked and the contents of the domain were re-directed through the person's web servers in the U.K., bogging them down and costing the web hosting company time and money.

E. Authentication

Though the Internet eliminates the need for physical contact, it does not do away with the fact that any form of contract or transaction would have to be authenticated.

Different authentication technologies have evolved over a period of time to ensure the identity of the parties entering into online transactions. However, there are some issues that need to be considered by companies.

- PKI AUTHENTICATION

Digital Signature is used as authentication tool. IT Act stipulates that digital signatures should be used for the purposes of authenticating an electronic contract.

The digital signature must follow the Public Key infrastructure ("PKI"). This acts as a limitation on the use of any other technology for authentication purposes. If Indian ecommerce companies use some other form of authentication technology, it could be said that there has been no authentication at all. [2]

F. Inter-Operable Standards

Laws of different countries provide different authentication standards, sometimes specifying a clear technology bias. These different authentication standards need to be inter-operable so as to facilitate cross-border transactions. This would need a high degree of co- operation between countries and the technology providers.

For example, an e-commerce company that uses PKI authentication technology for online contracts with Indian consumers may use different / other forms of technology while entering into online contracts with consumers in other countries.

In such a case, these contracts with foreign consumers may not be recognized in India as the authentication technology used is not PKI. However, such contracts may be enforceable in the foreign jurisdiction depending upon the laws of the foreign country.

G. Privacy & Data Protection

An important consideration for every e-commerce website is to maintain the privacy of its users. Some of the important privacy concerns over the Internet include:

Dissemination of sensitive and confidential medical, financial and personal records of individuals and organizations; sending spam (unsolicited) e-mails; tracking activities of consumers by using web cookies; and

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

unreasonable check and scrutiny on an employee's activities, including their email correspondence.

- DATA PROTECTION- SEC 43 A [3]
- SEC 43A -Compensation for failure to protect data
- If body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.
- The term "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities
- Liability – Damages by the way of compensation
- SENSITIVE PERSONAL INFORMATION OR DATA comprises of Passwords, Financial Information, Biometrics, Sexual Orientation, Medical and Health Records.

H. *Intellectual Property Rights (IPR)*

One of the foremost considerations that any company intending to commence ecommerce activities should consider is protection of its intellectual assets. Internet is a boundless and unregulated medium and therefore the protection of intellectual property rights ("IPRs") is a challenge and a growing concern amongst most e-businesses.

IPR ISSUES

DETERMINING SUBJECT MATTER OF PROTECTION

ASCERTAINING ORIGINALITY

ENFORCING IPR

PREVENTING UNAUTHORIZED HYPERLINKING & META TAGS- Courts in certain jurisdictions have held that hyper linking; especially deep-linking may constitute copyright infringement, whereas meta tagging may constitute trademark infringement.

I. *Domain Name Disputes*

A company that commences e-commerce activities would at first have to get its domain name registered. While registering domain names, if the company chooses a domain name that is similar to some domain name or some existing trademark of a third party, the company could be held liable for cyber squatting.

J. *Jurisdiction*

In e-commerce transactions, if a business derives customers from a particular country as a result of their website, it may be required to defend any litigation that may result in that country.

As a result, any content placed on a website should be reviewed for compliance with the laws of any jurisdiction; where an organization wishes to market, promote or sell its products or services as it may run the risk of being sued in any jurisdiction where the goods are bought or where the services are availed of.

The fact that parties to a contract formed through the Internet may be located in different jurisdictions may have implications for the interpretation and enforcement of the contract.

Therefore, a company should insert appropriate choice of law and choice of forum clauses in its online contract, which should specify the jurisdiction to which the parties to the contract would be subject to. Such clauses have been held by courts to be binding upon the parties.

K. *Liability*

The Internet knows no boundaries; the owner of a website could be confronted with legal liability for non-compliance or violation of laws of almost any country. Liability may arise due to various activities like invasion of privacy, trademark, copyright infringement, fraud, libel and defamation etc.

L. *Taxation*

Absence of national boundaries, physical presence of goods and non-requirement of physical delivery, taxation of e-commerce transactions raises several issues

They have to be understood in the light of International Taxation.

International Taxation arises from cross border transactions for the reason that author of transactions arises in one called Home State and the sites of the transactions is in the other country called Host State .

In e-commerce transactions, the contracting parties are in two different states and therefore, the question would arise as to which law would be applied.

V. Trends & Challenges- E-Commerce

The trends & challenges in E-commerce can be explained as:-

1) M-Commerce

M-commerce, or mobile commerce, is the next generation of e-commerce. This allows the buying and selling of goods through wireless hand-held devices such as mobile phones and PDA's. Consumers and enterprises can complete transactions without having to plug in to the internet. This wireless capability is made possible by WAP (wireless application protocol) technology.

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

- LEGAL CHALLENGES – M-COMMERCE

❖ When a person uses his/ her mobile to submit or confirm a purchase order or when a seller sells goods and services through portals allocated to receive requests from wireless devices via specific network providers, the resulting interrelationship between various parties poses many legal questions concerning

❖ Nature of relationships

❖ How should they be regulated

❖ Who can regulate

a) Contracts

Among the legal issues, which need to be considered, are the various forms of m-commerce.

- Identifying the contracting parties, their legal capacity to contract
- When the contract will be formed
- How they can be proved
- Other traditional issues of e-commerce contracts

b) Payment Issues & Jurisdiction

Another legal challenge is determining the method of payment. An important aspect which needs a thought is

- Applicable law

Courts having jurisdiction in disputes arising from use of mobile to transact business and conclude m-commerce contracts.

c) Privacy

Mobiles and allied technology conveys a lot of information about the user to the network provider who is able to pinpoint the user's where about. Companies can purchase such information, which may lead to breach of privacy. Privacy is another issue which requires legal framework

d) IPR- Intellectual Property Rights

A mobile user can use a digital camera installed on a wireless device to take photos, exchange with others and send them over internet. This may, if done without authorization result in infringement of intellectual property rights including copyright.

e) Crimes

Wireless networks are prone to attacks and carry a crime risk. Hackers can steal and erase information and data from mobiles, disrupt wireless networks. Virus also is another issue which infects mobiles and data residing therein. Key question is whether criminal laws would apply for these types of crimes and how will the penalties be enforced.

2) Social Commerce

It is a subset of e-commerce wherein social media assists in online buying and selling of products and services. Today, the area of social commerce has been expanded to include the range of social media tools and content used in the context of e-commerce. In simple words, it is the use of social network(s) in the context of e-commerce transactions.

It also encompasses other social shopping tools, such as forums and communities that allow buyers and sellers to discuss their online shopping experiences and compare transactional information.

- 6C's of Social Commerce
  - CONTENT
  - CONTEXT
  - COMMUNITY
  - CONVERSATION
  - COMMERCE
  - CONNECTION
- LEGAL CHALLENGES- SOCIAL COMMERCE
  - Social commerce is an adaptable means of selling to and engaging with customers. But in developing a strategy to fit, retailers need to consider a few key areas to make sure the business is social-commerce compliant.
  - Social commerce demands connection with customers on the go via mobile apps, so it raises the issues of privacy and data protection. Apps can access an array of information such as the user's location via GPS, browsing history, photo albums and social networking site profiles.
  - Companies should ensure that their data protection and privacy policies in relation to mobile applications are carefully drafted and up-to-date with current developments and that users can easily access, understand and amend the privacy settings. All social web platforms have special guidelines. This is especially important for running promotions, sweepstakes and contests.

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

VI. Cyber Crime Challenges to E-Commerce

A strong legal backup is also required to support all types of virtual contracting as well as transactions between parties for success in e-commerce. There must be national laws, in tandem with international laws and conventions, to boost e-commerce through passing relevant laws and establishing regulatory bodies. Some of these challenges include low levels of Internet penetration and limited legal support system.

India has made some progress in legalizing the electronic contracts format and electronic transactions through authentication of the electronic documents and records. To prevent misuse of the Internet in e-Commerce there are some Indian laws are already in place to tackle cyber crime into its cyber law with stipulated punishment in the form of imprisonment and fines.

The elementary challenges which are faced by cyber crime legislations are also shared by the e-commerce arena. These issues are:-

Jurisdiction is a tricky issue as far as the scene of crime and the origin of the accused are concerned.

It is the highly debatable issue as to the maintainability of any suits which has been filed. With increasing number of trans-border cyber crime the concept of territorial jurisdiction as envisaged under S.16 of C.P.C. and S.2.of the I.P.C. are put to question.

Loss of evidence is another crucial issue in cyber crime law enforcement as crucial data are destroyed by the perpetrators in seconds and without a trace. Further collection of data from another location in another country also makes it more difficult to prosecute the offenders.

VII. Provisions of IT Act – Extra Territorial

Though S.75 of IT Act provides for extra-territorial operations of this law, but these should be enforced with orders and warrants of external authorities and demands a highest level of inter-agency cooperation. Hence, cyber oriented lawyers and judges are another critical capacity building issue for enforcing cyber laws in any country.

The Information Technology Act, 2000, in India which makes the e-commerce site operator solely responsible for any action buyers and sellers take on an e-commerce market-place. Information Technology Act, 2000 undermines the promise of the e-commerce market-place - a faster, cheaper way of buying and selling products and services.

VIII. Conclusion

India is one of the few countries across the globe that has enacted e-commerce legislation. Effective risk management strategies coupled with adequate legal documentation will go along way in protecting e-commerce companies.

Though the Internet is a goldmine, without adequate legal protection it could become a landmine. The concept of commerce has been revolutionarized by technology by way of e-commerce. E-commerce has moved a step forward towards m-commerce, social commerce.

References

[1] http://www.cyberlawindia.com/
[2] http://www.cyberlawdb.com/main/
[3] http://www.cyberlaws.net

About Author :

Mr. S. Sai Sushanth is a Cyber Law Expert & Techno Legal Consultant. His expertise includes Information Technology Law, Cyber Law, Cyber Security, Cyber Forensics, Mobile Law, Cloud Computing Law, E-Commerce and Cyber Security Incident Response. He has published many papers in various International Journals and also is invited as a speaker to many International and National Conferences.